Symantec Mail Security™ for SMTP

Symantec Mail Security™ for SMTP

Documentation version 4.1

Copyright Notice

Trademarks

Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/ function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Symantec Software License Agreement
Symantec Mail Security™ for SMTP

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use the number of copies of the Software as have been licensed to You by Symantec under a License Module. If the Software is part of a suite containing multiple Software titles, the number of copies You may use may not exceed the aggregate number of copies indicated in the License Module, as calculated by any combination of licensed Software titles. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single computer;
B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;
D. use the Software in accordance with any written agreement between You and Symantec; and
E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

You may not:

A. copy the printed documentation that accompanies the Software;
B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
D. use a previous version or copy of the Software after You have received and installed a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
E. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;
F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received permission in a License Module; nor
G. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; antispam software utilize updated antispam rules; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to

designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of thirty (30) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. Licensee agrees to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

8. Additional Uses and Restrictions:

A. If the Software You have licensed is Symantec Mail Security for a corresponding third party product or platform, You may only use that Software for the corresponding product or platform. You may only use the Software for the number of users set forth in the License Module.

B. If the Software You have licensed is Symantec Premium AntiSpam, the following terms and conditions apply:

1.You may use the Software in the quantity licensed to You by Symantec under a License Module until the end date indicated on the License Module ("the End Date"), solely on computing devices owned by you, to filter incoming email sent to Your End Users on Your Email Service;

2.You must have a license for each End User for whom you use the Software to filter email. "End User" means an employee, contractor or other agent authorized by You as a user of an email mailbox account or an email address hosted by Your Email Service. "Email Service" means Your email services provided to End Users for the purposes of conducting Your internal business and which are enabled via Your mail transfer agent;

3.You may copy the Software onto Your computing devices as necessary to exercise the rights granted in Section B.1, above; and

4.You may not use the Software after the End Date.

C. If the Software You have licensed is Symantec Premium AntiSpam, the following additional terms apply to Jikes, a third party technology associated with the Software:

1.Licensee is entitled to a copy of the source code for Jikes from http://www-124.ibm.com/developerworks/downloads/detail.php?group_id=10&what=rele&id=501. The use of Jikes is governed by the IBM Public License, the full text of which can be found at http://www-124.ibm.com/developerworks/opensource/license10.html (the "IBM License").

2.OTHER THAN AS PROVIDED IN THIS AGREEMENT, THE CONTRIBUTORS (AS DEFINED IN THE IBM LICENSE) MAKE NO REPRESENATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY (EITHER IN FACT OR BY OPERATION OF LAW), AND EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING WITHOUT LIMITATION, WARRANTIES OF TILTE AND NON-INFRINGEMENT, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

3.Other than as otherwise provided in this Agreement, in no event will any of the Contributors be liable for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits.

4.Any provisions in this License Agreement that differ from the IBM License are offered by Symantec alone and not by any other party.

Contents

Chapter 5 Setting your antispam policy

Chapter 6 Setting your filtering policy

Chapter 7 Logging and reporting

Chapter 8 Integrating Symantec Mail Security for SMTP with SESA

Chapter 1

Introducing Symantec Mail Security for SMTP

This chapter includes the following topics:

About Symantec Mail Security for SMTP

Symantec Mail Security for SMTP is a Simple Mail Transfer Protocol (SMTP) server that processes email before sending it to a local mail server for delivery. It can be configured to protect your network in the following ways:

- Block unwanted email messages.
- Scan and repair infected email attachments (files appended to email messages) and infected files within attachments.
- Block spam.
- Prevent the relaying of spam to another host.

The email gateway is only one way that a virus can penetrate your network. For comprehensive virus protection, install both Symantec Mail Security for SMTP and appropriate workstation or server versions of antivirus protection on every computer at your site.

For a complete listing of Symantec antivirus products, visit www.symantec.com.

What's new in Symantec Mail Security for SMTP

Table 1-1 lists the new features in Symantec Mail Security for SMTP.

Table 1-1 New features in Symantec Mail Security for SMTP

Feature	Description
Symantec Premium AntiSpam	The premium antispam service includes the following features: ■ Reputation service: Symantec monitors email sources to determine how much of the email that is sent from those sources is legitimate. Email from those sources can then be blocked or allowed based on the source's reputation value as determined by Symantec. ■ Language identification: Symantec can determine the language in which a filtered message is written. You can configure the premium antispam service to automatically send messages that are written in certain languages to a spam folder in the recipient's mailbox. To use this feature, you must deploy the optional plug-in for Microsoft Outlook to the desktop computers on your network. ■ URL filtering: Symantec builds its known-spammer list based on URLs that appear in spam. This list contains over 20,000 URLs. ■ Heuristic filtering: Heuristic filters scan the headers and the body of a message to test for characteristics that are usually inherent in spam, such as opt-out links, specific phrases, and forged headers. ■ Signature filtering: Messages that flow into the Symantec Brightmail Logistics and Operations Center (BLOC) are characterized using a unique signature that is added to the database of known spam. Using this signature, Symantec can group and match seemingly random messages that originated from a single attack.
Spam Quarantine	The spam quarantine stores messages that are identified as spam. An administrator account provides access to quarantined messages. Users can check the quarantine for misidentified messages, resend messages to their inbox, and delete or search messages. Users can access the spam quarantine through a Java-based Web server.

Components of Symantec Mail Security for SMTP

Symantec Mail Security for SMTP consists of several components that work together to protect your network.

Table 1-2 describes each component.

Table 1-2 Symantec Mail Security for SMTP components

Component	Description
Symantec Mail Security for SMTP	This is the software that you install to protect network servers and workstations. It protects computers from viruses in email attachments, blocks unwanted content, and prevents spam and spam relaying.
LiveUpdate™ Administration Utility	LiveUpdate lets Symantec products download program and virus definitions files updates directly from Symantec or from an intranet LiveUpdate server. The LiveUpdate Administration Utility lets you configure one or more intranet FTP, HTTP, or LAN servers to act as internal LiveUpdate servers. For more information, see the *LiveUpdate Administrator's Guide* on the product CD.
Symantec Central Quarantine	You can configure Symantec Mail Security for SMTP to automatically forward infected attachments from local quarantine servers to Symantec Central Quarantine, which is a central repository for infected attachments. You can configure Symantec Central Quarantine to automatically send files that it cannot repair to Symantec Security Response for analysis and repair. For more information, see the *Symantec Central Quarantine Administrator's Guide* on the product CD.
Java 1.3.1	This version of Java (or a later version) is required for LiveUpdate and the Symantec Enterprise Security Architecture (SESA). During installation, Symantec Mail Security checks for this software and stops the installation if it is not present.
Spam quarantine	You install the spam quarantine separately from the product. The spam quarantine lets users with Web access browse, search, and delete their spam messages and deliver misidentified messages to their inboxes. An administrator account provides access to all quarantine messages.

Table 1-2 Symantec Mail Security for SMTP components

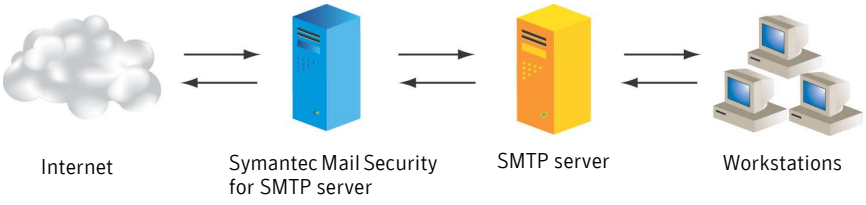
Component	Description
Microsoft® Outlook® Plug-in	As a part of the premium antispam service, this is the software that lets you submit missed spam and false positives to Symantec. It also lets you administer your own allowed senders and blocked senders lists and specify languages in which you do not wish to receive email.
Spam Folder Agent	As a part of the premium antispam service, this is the software that lets you automatically route spam messages to a spam folder in the recipient's mailbox. It installs a subfolder and a server-side filter in each user's mailbox of a Microsoft Exchange 2000 or Lotus Domino server.
Adobe® Acrobat® Reader®	This is the software that makes it possible to read documentation in PDF format.

How Symantec Mail Security for SMTP works

In a typical configuration, Symantec Mail Security for SMTP operates as an SMTP server that accepts incoming email from the Internet, processes the email based on the configuration of the product, and delivers the email to another SMTP server for further processing and delivery. It also receives outgoing email from your SMTP server and processes it based on the configuration of Symantec Mail Security for SMTP.

Figure 1-1 shows how Symantec Mail Security for SMTP is typically configured on a network.

Figure 1-1 Typical processing path for Symantec Mail Security for SMTP



When Symantec Mail Security for SMTP receives an email message with an attachment from an Internet or internal network source, it decodes and decompresses the message. It sends the message to the fast queue (a logical

queue with a large number of dedicated threads) to be processed. Symantec Mail Security for SMTP first looks for messages to block before scanning for viruses. You can configure Symantec Mail Security for SMTP to notify senders and administrators when messages are blocked.

After blocking messages, Symantec Mail Security for SMTP uses several antivirus technologies to scan remaining messages for viruses. It looks for known viruses by comparing file segments to the sample code inside of a virus definitions file. The virus definitions file contains nonmalicious bits of code, or virus definitions, for thousands of viruses. If Symantec Mail Security for SMTP finds a match, the file is considered infected, and the email is handled (repaired, deleted, or logged and delivered) according to how you have configured the software. To protect your network from new viruses, you can configure regular virus definitions file updates.

See "Updating virus and spam definitions files" on page 84.

By default, when Symantec Mail Security for SMTP detects a virus in an email attachment (that is not a container file), it attempts to repair the infected attachment. If Symantec Mail Security for SMTP cannot repair the attachment, it deletes the attachment by default. With container files, Symantec Mail Security for SMTP removes the infected files from the containers and attempts to repair the files. If a virus is detected, Symantec Mail Security for SMTP inserts text in the body of the message that specifies which virus was found and where it is located.

You can configure Symantec Mail Security for SMTP to forward infected messages to a Central Quarantine Server, and configure the Central Quarantine Server to automatically submit virus samples to Symantec Security Response for analysis.

After blocking and scanning messages, Symantec Mail Security for SMTP delivers them. If the message cannot be delivered, it is moved to the slow queue so as not to backlog the fast queue. Once the message is in the slow queue, a message is sent to the original message sender indicating that Symantec Mail Security for SMTP will continue to attempt delivery of the message.

Symantec Mail Security for SMTP reorders messages in the slow queue. Messages that cannot be delivered are moved to the rear of the queue. Queue messages that are destined to the same host on the next hop are moved to the front of the queue (if those hosts are accepting delivery). If the message is not able to be delivered within the specified number of days, Symantec Mail Security for SMTP returns a reason (for example, wrong domain, user name doesn't exist) to the original message sender, and the file is deleted from the slow queue.

What you can do with Symantec Mail Security for SMTP

Symantec Mail Security for SMTP handles messages and attachments according to your antivirus, antispam, and content filtering policies. You set your policies through the Symantec Mail Security for SMTP administrative interface, from either the physical server on which the software is installed or from any workstation on the network.

See "Setting your antivirus policy" on page 77.

See "Setting your antispam policy" on page 89.

See "Setting your filtering policy" on page 125.

You can configure Symantec Mail Security for SMTP so that users on the network become aware of its operation only if a virus or content violation is detected. You can also configure Symantec Mail Security for SMTP to send alerts to administrators in the case of system events, and send notifications to administrators and senders when there is virus activity.

See "Configuring alerts" on page 67.

Filter email messages

Your filtering policy is determined by how you configure Symantec Mail Security for SMTP to filter messages. You can specify which criteria to use to filter messages and attachments and how those filtered messages and attachments should be handled.

See "Setting your filtering policy" on page 125.

Symantec Mail Security for SMTP can be configured to filter messages based on the following:

- Message size
- Subject line
- File name
- Container limits
- Encrypted container
- Characters in email addresses
- Content rules

Identify spam

Your antispam policy is determined by how you configure Symantec Mail Security for SMTP to identify spam. You can specify which criteria to use to identify spam and how those messages should be handled.

See "Setting your antispam policy" on page 89.

Symantec Mail Security for SMTP can be configured to identify spam based on the following:

- Symantec Premium AntiSpam Service
  This service is sold and licensed separately from Symantec Mail Security for SMTP.
- Sender address
- Real-time blacklist antispam lists
- Heuristic detection
- Spam rules

Respond to viruses

Your antivirus policy is determined by how you configure Symantec Mail Security for SMTP to handle email messages (for example, which file types to scan, which messages to quarantine, and when to notify administrators and senders if viruses are found or virus outbreaks occur).

See "Setting your antivirus policy" on page 77.

Table 1-3 lists the options for handling infected attachments.

Table 1-3 Options for handling infected attachments

Option	Description
Repair	The virus within the attachment is repaired, if possible.
Delete	No repair is attempted. The attachment is deleted from the message.
Log only	No repair is attempted. The incident of a virus is logged, and the message is delivered.

Table 1-4 lists the options for handling unrepairable infected attachments.

Table 1-4 Options for handling unrepairable infected attachments

Option	Description
Delete	The attachment is deleted from the message.
Log only	The incident of a virus is logged, and the message is delivered.

Table 1-5 lists the options for handling attachments that are not repaired or deleted.

Table 1-5 Options for handling attachments that are not repaired or deleted

Option	Description
Drop message	Email messages that contain unrepairable infected attachments that were not deleted are dropped.
Log only	A record of the incident is logged and the message is delivered.

Table 1-6 lists the quarantine options for infected messages.

Table 1-6 Quarantine options

Option	Description
Quarantine nothing	No files are quarantined.
Quarantine messages containing unrepaired infections	Copies of messages that contain attachments that cannot be repaired are quarantined. **Note:** This option is available only if you have enabled scanning in Symantec Mail Security for SMTP.
Quarantine all messages containing attachments	Copies of all infected messages are quarantined. **Note:** This option is available only if you have enabled scanning in Symantec Mail Security for SMTP.

Configure relay settings

Symantec Mail Security for SMTP works with other email software products that are running on other local mail servers. After processing messages, Symantec Mail Security for SMTP relays the messages to mail servers according to how you have configured your relay settings.

See "Configuring routing options" on page 62.

By establishing anti-relay settings, Symantec Mail Security for SMTP prevents the relaying of spam by an external host.

See "Preventing relaying" on page 135.

Notify senders and administrators of policy violations

Symantec Mail Security for SMTP lets you customize notifications for administrators and senders when any of the following occur:

- Virus repaired
- Virus not repaired
- Content deleted
- Content not deleted
- Container limit dropped
- Encrypted container altered or deleted

Chapter 2

Installing Symantec Mail Security for SMTP

This chapter includes the following topics:

Before you install

You must perform the following pre-installation tasks when appropriate:

- Install and configure the operating system.
  See "Installing and configuring the operating system" on page 24.
- Upgrade from earlier versions of Symantec Mail Security for SMTP.
  See "Upgrading from previous versions" on page 24.
- Configure DNS.
  See "Configuring DNS" on page 25.

- Prevent conflicts with other SMTP servers.
  See "Preventing conflicts with other SMTP servers" on page 26.
- Prevent conflicts with other software.
  See "Preventing conflicts with other software" on page 27.
- Prevent conflicts with Symantec Web Security.
  See "Preventing conflicts with Symantec Web Security (Solaris only)" on page 27.

Installing and configuring the operating system

The operating system software and applicable updates must be installed, configured, and working correctly on your server before you install Symantec Mail Security for SMTP.

For more information, see your server's documentation.

Upgrading from previous versions

To upgrade from Symantec AntiVirus for SMTP Gateways 3.0 or 3.1 or Symantec Mail Security for SMTP 4.0, you should install Symantec Mail Security for SMTP 4.1 over the existing software. This lets you retain settings from the previous version.

The | (pipe) symbol is no longer allowed in the Include, Exclude, and Attachment Stripping lists when configuring scan options. Symantec Mail Security for SMTP removes the symbol during the upgrade.

Note: If you are installing over a Symantec AntiVirus for SMTP Gateways installation that had file extension entries that were not preceded by a period (.), Symantec Mail Security for SMTP automatically adds the period. For example, if exe was in the Include list of the previous version, Symantec Mail Security for SMTP changes it to .exe to the force the configuration into compliance with the standard for file extension formats.

Preserving configuration settings from previous versions that use high ASCII or DBCS directories

Version 4.1 does not support high ASCII or DBCS characters in directory names. If you have used high ASCII or DBCS characters for directories in your previous version of Symantec Mail Security for SMTP, you must back up the configuration file for the previous version and copy the file into version 4.1.

To preserve configuration settings from previous versions that use high ASCII or DBCS directories

1. Stop the Symantec Mail Security for SMTP 4.0 service.
2. Back up the queues, logs, and local folders.
   If these files are not backed up, queued mail and logging information will be deleted, and configuration settings will be lost.
3. Uninstall the previous version.
4. Delete the installation directory that is left behind after the installation.
   There is usually one directory in Windows. There may be multiple directories in Solaris.
5. Create a directory for the backed-up queues, logs, and local folders where the new version will be installed.
   For Windows, the default directory is C:\Program Files\Symantec\SMSSMTP\
   For Solaris, the default directory is /var/opt/SMSSMTP/
6. Copy the backed up queue, log, and local folders into the directory that you created.
7. Install Symantec Mail Security for SMTP 4.1.
   Be sure to specify during installation the directory that was created for the backed-up folders.

Configuring DNS

Symantec Mail Security for SMTP works with other SMTP mail servers. By properly configuring your site's domain name system (DNS), messages that are destined for your existing mail server arrive at Symantec Mail Security for SMTP first. After scanning for viruses, Symantec Mail Security for SMTP forwards the message to your SMTP server for delivery.

The DNS zone for your site must be configured to support reverse name lookup, which is used to verify the IP address of the host or domain that you are trying to resolve.

Symantec Mail Security for SMTP processing is affected when you modify DNS records. The following types of records are involved in the delivery of messages:

A record	A mapping of host names to IP addresses. For example, the host name www.somewhere.com might map to the specific IP address 192.168.23.10.
PTR record	A mapping of IP addresses to host names.
MX record	A mapping of domains to mail exchange host names. Any message that is sent to a particular user at a domain (such as user@somewhere.com) is resolved by a DNS server MX record to a host name, such as mailer.somewhere.com. Then, the A record resolves the name mailer.somewhere.com to an IP address.

Contact your administrator or Internet service provider (ISP) if you are unsure of how to configure DNS records.

Note: You can modify DNS so that the MX record points to the firewall, in which case the firewall would route traffic internally. In this scenario, changes are made to the firewall rather than to the MX record.

Preventing conflicts with other SMTP servers

Because Symantec Mail Security for SMTP is an SMTP server, it must have exclusive access to the TCP/IP port that corresponds to that service. No other SMTP servers can be running on the same port on the same server on which Symantec Mail Security for SMTP is installed. You must stop these conflicting services before installing Symantec Mail Security for SMTP.

Note: When you install Symantec Mail Security for SMTP on a Solaris™ server, the installation program may detect conflicting programs that are commonly found on Solaris (such as the Solaris Sendmail™ program, which runs on port 25). If such programs are detected, Symantec Mail Security for SMTP returns an error message. Therefore, you should stop the conflicting programs before installing Symantec Mail Security for SMTP.

Preventing conflicts with other software

You must stop any other antivirus software on the server on which Symantec Mail Security for SMTP will be installed. After installation, reenable the antivirus protection.

If another file-system antivirus product is installed on the Symantec Mail Security for SMTP server (for example, Symantec AntiVirus Corporate Edition), the competing product may try to scan and delete Symantec Mail Security for SMTP files that are placed in the Queues directory and temporary directory during its scanning process.

Note: If you are running a desktop antivirus product on the server on which you install Symantec Mail Security for SMTP, you must configure the desktop product not to scan the Queues directory and the temporary directory that is used by Symantec Mail Security for SMTP. Scanning these directories will cause significant operational problems with the software.

Preventing conflicts with Symantec Web Security (Solaris only)

If Symantec Web Security and Symantec Mail Security for SMTP are installed on the same Solaris server, LiveUpdate must be run independently for each product to avoid a conflict. Run LiveUpdate first for one product, and then for the other to obtain the latest definitions for both products.

See "To schedule automatic LiveUpdates" on page 84.

System requirements

You must have root or local administrator-level privileges to install Symantec Mail Security for SMTP. You should install Symantec Mail Security for SMTP on its own server.

The system requirements for Solaris and Windows 2000/2003 Server are as follows:

Operating system	■ Solaris 8 or 9 ■ Windows 2000 Server with Service Pack 4/Windows Server 2003
Processor	■ Solaris: UltraSPARC®-based server ■ Windows 2000/2003 Server: Intel® Pentium® or compatible
Memory	■ 512 MB RAM (1 GB or more recommended for optimal performance)
Disk space to install	■ 100 MB
Available disk space after installation for email processing	■ 500 MB minimum
Network configuration	■ Static IP address for the computer that will run Symantec Mail Security for SMTP ■ TCP/IP Internet connection ■ Appropriately configured DNS to include Address (A), Pointer (PTR), and Mail eXchange (MX) records for your servers ■ DNS zone for your site that is configured to support reverse name lookup
Internet browser	■ Netscape Navigator version 7.02 or later ■ Microsoft Internet Explorer version 6.01 or later
Other software	■ Java 1.3.1 or higher (needed for LiveUpdate and SESA) This version of Java is located on the product CD.

Installing Symantec Mail Security for SMTP

Note: You should install Symantec Mail Security for SMTP on a separate server from your SMTP server to avoid significant impact on network resources.

You need root or administrator-level privileges to install Symantec Mail Security for SMTP. A static IP address is required.

If you decide to install Symantec Mail Security for SMTP on the same computer as your SMTP server, you must configure Symantec Mail Security for SMTP to listen on the port to which mail clients deliver messages. Because port 25 is the port to which most servers send email connection requests, you should configure Symantec Mail Security for SMTP listen on port 25. If your mail server is currently listening on port 25, you must change your server to listen on a different port.

On Solaris, if another process is running on port 25, Symantec Mail Security for SMTP automatically attempts to disable it. A record that the process has been disabled is placed in the log directory. If another process is disabled because it is running on port 25, there is an on-screen option during installation that lets you stop the installation process and change the port for the existing process or allow Symantec Mail Security for SMTP to disable the process and continue the installation on port 25.

Note: If another process that is running on port 25 is disabled, you must configure the disabled process to run on another port.

Complete the following tasks in the order in which they are listed to install Symantec Mail Security for SMTP:

- Verify that DNS is properly configured for your network.
  See "Verifying and testing DNS settings" on page 30.
- Run the installation script or setup program.
  See "Running the installation script or setup program" on page 31.
- Specify locations for installation directories.
  See "Specifying locations for installation directories" on page 32.
- Select an HTTP server port.
  See "Selecting an HTTP server port" on page 34.
- Select an HTTPS server port.
  See "Selecting an HTTPS server port" on page 35.

Verifying and testing DNS settings

Your server must be configured as a DNS client before installing Symantec Mail Security for SMTP.

Verify and test DNS settings

To verify DNS settings, you must check the TCP/IP properties for your server. To test your DNS server, use the Name Server Lookup (NSLookup) utility.

To verify DNS settings on Windows 2000/2003 Server

1. Open Local Area Connection Properties.
2. Click **Internet Protocol (TCP/IP)**.
3. Click **Properties**.
4. Click **Advanced**.
5. On the DNS tab, specify the domain suffix and verify that at least one valid DNS server is listed in the DNS server addresses list.
   The host name is the Computer name that is entered in System Properties on the Network Identification tab.
   Contact your administrator or Internet service provider (ISP) if you are unsure of the values to use.

To verify DNS settings on Solaris

1. Open the following file:
   /etc/resolv.conf
   The file should contain lines similar to the following:
   domain somewhere.com
   nameserver 192.168.1.2
   nameserver 192.168.9.7
   Verify that the specific domain name and name server addresses are correct for your site.
   Contact your administrator or Internet service provider (ISP) if you are unsure of the values to use.
2. Make any necessary changes.
   If the /etc/resolv.conf file does not exist on your server, create it using the example in step 1 as a template. Replace the domain name and name server addresses with values that are correct for your site.

To test your DNS server

- Run the NSLookup command using the following format:
  nslookup <IP address or server name>
  For example, nslookup 155.55.55.55
  The IP address should resolve to your server name and the server name should resolve to your IP address.

Note: You should run NSLookup twice (once in the format nslookup <host name> and once as nslookup <IP address>).

Running the installation script or setup program

You must run the installation script (Solaris) or setup program (Windows 2000 Server) to install Symantec Mail Security for SMTP.

Run the installation script or setup program

The Symantec Mail Security for SMTP files are included on the installation CD.

For Solaris, you must be logged on as root.

For Windows 2000/2003 Server, you must be logged on with administrator privileges.

To run the Symantec Mail Security for SMTP installation script on Solaris

1. Change (cd) to the location of the installation files.
2. Type the following command to run the installation script:
   sh smssmtp.sh
3. Follow the on-screen instructions.
   A transcript of the installation is saved as /var/log/SMSSMTP-install.log for later review, if necessary.
4. Verify that the software is running by viewing the Status page.
   The Date server started field should be current.
   See "About the Status page" on page 141.

To run the Symantec Mail Security for SMTP setup program on Windows 2000/2003 Server

1. Change (cd) to the location of the installation files.
2. Run Setup.exe.
3. Follow the on-screen instructions.
4. Verify that the software is running by viewing the Status page.
   The Date server started field should be current.
   See "About the Status page" on page 141.

Specifying locations for installation directories

Symantec Mail Security for SMTP is organized into directories that each contain specific kinds of files.

The location of each directory can be specified during installation, during which a default location is shown. You should accept the default location.

Table 2-1 shows the default installation directory locations for Solaris.

Table 2-1 Installation directories for Solaris

Directory	Description	Default location
InstallDir	Contains the Symantec Mail Security for SMTP program files and read-only data files. At least 1200 MB disk space is required.	/opt/SMSSMTP Antivirus and antispam files: at /opt/SMSSMTP/CSAPI/ AntiVirus (or AntiSpam)
MailDir	Contains SMTP queue files. At least 500 MB disk space is recommended.	/var/opt/SMSSMTP/queues
LocalDir	Contains server-specific configuration files. At least 1 MB disk space is required.	/var/opt/SMSSMTP/local
LogDir	Contains log files that record Symantec Mail Security for SMTP activity. At least 600 MB disk space is recommended.	/var/opt/SMSSMTP/logs
DiagDir	Contains files that can help Symantec technicians address issues that may arise with the software. At least 34 MB disk space is recommended.	/var/opt/SMSSMTP/queues/ diagnosticfiles

Table 2-1 Installation directories for Solaris

Directory	Description	Default location
ScanDir	Contains temporary files that are created during Symantec Mail Security for SMTP scanning. At least 100 MB disk space is recommended. **Note:** Files in the ScanDir are deleted after scanning.	/tmp/smssmtptemp
DocsDir	Contains the readme file, license agreement, and a PDF version of the *Symantec Mail Security for SMTP Implementation Guide*. At least 1 MB disk space is recommended.	var/opt/SMSSMTP/manuals/<language>
CSAPIDir	Contains the decomposer, premium antispam, antivirus, and heuristic antispam files.	/opt/SMSSMTP/csapi

Table 2-2 shows the Windows default installation directory locations.

Table 2-2 Installation directories for Windows

Directory	Description	Default location
Install	Contains the Symantec Mail Security for SMTP program files and read-only data files. At least 1200 MB disk space is required.	\ProgramFiles\Symantec\SMSSMTP
Queues	Contains SMTP queue files. At least 500 MB disk space is recommended.	\ProgramFiles\Symantec\SMSSMTP\queues
Local	Contains server-specific configuration files. At least 1 MB disk space is required.	\ProgramFiles\Symantec\SMSSMTP\local
Logs	Contains log files that record Symantec Mail Security for SMTP activity. At least 600 MB disk space is recommended.	\ProgramFiles\Symantec\SMSSMTP\logs

Table 2-2 Installation directories for Windows

Directory	Description	Default location
Diagnostic	Contains files that can help Symantec technicians address issues that may arise with the software. At least 34 MB disk space is recommended.	\ProgramFiles\Symantec \SMSSMTP\queues\ diagnosticfiles
Docs	Contains the readme file, license agreement, and a PDF version of the *Symantec Mail Security for SMTP Implementation Guide*. At least 1 MB disk space is recommended.	\Program Files\Symantec\SMSSMTP\ docs\<language>
CSAPI	Contains the decomposer, premium antispam, antivirus, and heuristic antispam files.	\ProgramFiles\Symantec\ SMSMTP\csapi

Selecting an HTTP server port

Symantec Mail Security for SMTP is managed through a Web-based interface. This interface is provided through a built-in Hypertext Transfer Protocol (HTTP) server that is included with Symantec Mail Security for SMTP. This HTTP server is independent of any existing HTTP server that may already be installed on your server and is not a general-purpose Web server.

During the installation process, you are prompted for the TCP/IP port number on which this built-in HTTP server will listen. The number that you specify becomes the port number in the URLs that you use to access the Symantec Mail Security for SMTP interface. The port number that you specify must be different from the HTTPS and SMTP port numbers, exclusive to Symantec Mail Security for SMTP, and not already in use by any other program or service.

Because the built-in HTTP server is not a general-purpose Web server, do not use port number 80 (the default port number for general-purpose Web servers). You should use the default port number of 8003. If you select a port number other than the default, remember which port number you selected.

Selecting an HTTPS server port

HTTPS stands for HTTP via Secure Sockets Layer (SSL). With HTTP, all information is sent in clear text with no authentication between the client and server. With HTTPS, there is client and server authentication using a certificate that has been signed by a Certificate Authority. Once a legitimate Web certificate is installed on the server that is running Symantec Mail Security for SMTP, the server and client share a common key that lets them encrypt and decrypt messages that they send to each other. In Symantec Mail Security for SMTP, secure connections are used for the logon- and password-changing portions of the administrative interface, when they are enabled.

During installation, you must identify the TCP/IP port number on which the HTTPS server will listen. The port number that you specify must be different from the HTTP and SMTP port numbers, exclusive to Symantec Mail Security for SMTP, and not already in use by any other program or service. The default HTTPS port number is 8043. You should select the default.

Note: You must identify an HTTPS port number during installation even if you do not enable SSL.

About the Symantec Plug-in for Outlook

The Symantec Plug-in for Outlook lets Microsoft users submit missed spam and false positives to Symantec. Depending on how you configure the plug-in, user submissions can also be automatically sent to a local administrator. The plug-in for Outlook also lets you administer your own blocked senders and allowed senders lists and specify languages in which you do not wish to receive email.

You can install the plug-in from the Symantec Mail Security for SMTP CD. The plug-in adds a toolbar to the Outlook window from which users can access the help system.

Note: Do not install the plug-in on the server on which Symantec Mail Security for SMTP is installed.

The plug-in can be used with Outlook 2000/2002/XP/2003 on Windows 98/Me/NT/2000/XP.

Installing the Symantec Spam Folder Agent

The Symantec Spam Folder Agent lets you automatically route spam messages to a spam folder in the recipient's mailbox. The agent creates a subfolder and a server-side filter in each user's mailbox on a Microsoft Exchange or Lotus Domino server. This filter is applied to each message that is identified as spam or suspected spam, and the identified message is routed to a user's spam folder. If the agent detects that the user's spam folder has been deleted or moved, it recreates the subfolder.

You can install the Symantec Spam Folder Agent from the Symantec Mail Security for SMTP CD.

Note: You must install the agent on the server on which Symantec Mail Security is installed.

To install the Symantec Spam Folder Agent

1. On the product CD, click **Install Spam Folder Agent**.
2. Read the license agreement, click **I accept the terms of this license agreement**, and then click **Next**.
3. Select one of the following setup types, and then click **Next**.

Complete	Installs all software in a predefined set of folders and files
Custom	Lets you tailor installation options

4. Under Service Account, specify an account to be used by the agent. Type the Active Directory or NT Domain and the user name and password.
   The account must have full access to the mailbox that is specified in the Mailbox box.
5. In the Mailbox box, type the mailbox alias of a valid mailbox for the agent to use.
   To find this alias, click **Active Directory Users and Computers**, right-click **User properties**, and then click the **General** tab.
6. In the **Spam expiration** box, select the number of days that you want to retain spam messages, and then click **Next**.
   The default is 30 days.

7 Click **OK**.

8 Click **Install** to begin the installation process.

9 Click **Finish**.
The Installer configures the spam folder agent as a Windows service that runs automatically.

Post-installation tasks

You must perform the following post-installation tasks when appropriate:

- Access the administrative interface.
See "Accessing the administrative interface" on page 37.
- Activate a product and content license.
See "Activating product and content licenses" on page 38.
- Route scanned email for delivery.
See "Routing scanned messages for delivery" on page 40.
- Stop and restart Symantec Mail Security for SMTP.
See "Stopping and restarting Symantec Mail Security for SMTP" on page 41.

Accessing the administrative interface

You must access the administrative interface to configure Symantec Mail Security for SMTP.

Access the Symantec Mail Security for SMTP administrative interface

You can access Symantec Mail Security for SMTP through a browser window, from the Start menu, or by clicking the desktop icon (if it is running in Windows).

To access the Symantec Mail Security for SMTP administrative interface through a browser window

1. Open your browser.
2. Type the Symantec Mail Security for SMTP IP address or host name using the following format:
   http://<IP address or host name of the computer that is running the software>:<port number>
   For example, use either of these formats:
   http://smssmtp.somewhere.com:8003
   http://198.0.0.1:8003
3. Log on using the password that you set during installation.
   Passwords are case-sensitive.

To access the Symantec Mail Security for SMTP administrative interface through the Start menu

- On the Windows taskbar, click **Start** > **Programs** > **Symantec Mail Security for SMTP**.

Activating product and content licenses

You must install a license file on each server that is running Symantec Mail Security for SMTP in order to activate your product and content licenses. The product license is required to activate Symantec Mail Security for SMTP scanning operations. The content license is required to receive the latest virus and heuristics spam definitions updates. To install a license file, you must have the serial number that is required for activation. The serial number is listed on your license certificate.

The product certificate is mailed separately from the software and is needed to request a license file and to register for support. The license certificate should arrive at approximately the same time that you receive the software. (It may be sent to you by email if that method has been requested). The format of a serial number is a letter followed by 10 digits, for example: F2430482013.

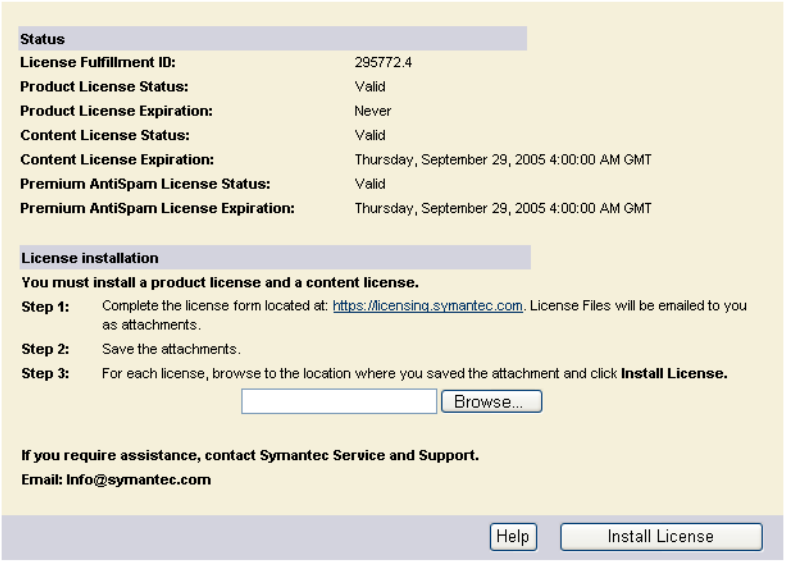
If you purchased Symantec Premium AntiSpam when you purchased Symantec Mail Security for SMTP, this serial number is listed on the license certificate. This serial number is needed to receive the latest spam definition updates for the premium antispam service. If you purchased only Symantec Premium AntiSpam, only the serial number that is needed to activate that license is listed.

After the license files are installed, content and spam updating is enabled for the duration of your maintenance contract. When a content or spam license expires, a new license must be installed to renew the subscription. When no license is installed, virus and spam definitions that are needed to keep protection current are not downloaded.

If you have questions about licensing, contact Symantec Customer Service at 800-721-3934 or your reseller to check the status of your order.

To activate product and content licenses

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Licensing.**



2 On the License Management page, under License installation, follow steps 1, 2, and 3 on the administrative interface to acquire license files from Symantec.

3 On the administrative interface, in step 3, do one of the following:

- Type the fully qualified path to the License File, and then click **Install License**.
  If the License File does not reside on the same computer, you can specify a mapped drive or UNC path to the file.
- Click **Browse**, select the License File, and then click **Install License**.
  If the License File does not reside on the same computer, you can locate the file using My Network Places.
  You can install the content and Symantec Premium AntiSpam license one after the other.

Routing scanned messages for delivery

You must add a routing list entry for each serviced email domain on your network.

If the Symantec Mail Security for SMTP server is not the last hop before the Internet, you might need to use default routing.

See "Configuring default routing" on page 62.

To route scanned messages for delivery

1 Open Symantec Mail Security for SMTP.

2 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.

3 On the Routing tab, under Local Routing List, click **Add**.

4 Under Routing list entry, in the Host or Domain box, type the domain of your incoming mail server (for example, if your email address is admin@brightcorp.com, type brightcorp.com).

5 Under Destination relay, in the Host box, type the fully qualified domain name or IP address of your mail server.

6 In the Port box, type the port number of your mail server.

7 Click **Save**.
All mail that was previously destined for your SMTP server goes to Symantec Mail Security for SMTP for processing, and then is forwarded to your SMTP server for delivery.

Stopping and restarting Symantec Mail Security for SMTP

You may need to stop and restart Symantec Mail Security for SMTP. Stopping and restarting the service results in a lost connection to client applications that may be submitting a file for scanning or delivery. The client application must reestablish the connection and resubmit the file for scanning and delivery.

Note: If messages are being processed when the service is stopped, the processing of those messages stops and resumes when the service is restarted.

Stopping and restarting Symantec Mail Security for SMTP

Instructions for stopping and restarting Symantec Mail Security for SMTP differ depending on the operating system that you are running. If you are running Symantec Mail Security for SMTP on Windows 2000/2003 Server, stop and restart the service in the Services Control Panel.

To stop Symantec Mail Security for SMTP on Solaris

- Type the following command:
  /etc/init.d/smssmtp stop

To restart Symantec Mail Security for SMTP on Solaris

- Type the following command:
  /etc/init.d/smssmtp start

Uninstalling Symantec Mail Security for SMTP

There are different instructions for uninstalling Symantec Mail Security for SMTP from Solaris and Windows.

Uninstall Symantec Mail Security for SMTP from Solaris

If Symantec Mail Security for SMTP was permitted to automatically disable conflicting services when it was installed, an attempt will be made during the uninstallation process to reenable those services.

There may be files and registry entries that are not removed when you uninstall Symantec Mail Security for SMTP. You must manually delete those files and entries.

Warning: If you are running other Symantec products, certain shared files, such as registry files, should not be deleted.

To uninstall Symantec Mail Security for SMTP from Solaris

- Type the following command:
  pkgrm SYMCsmtp

To manually delete files and registry entries that are left behind after uninstallation

- Type the following commands:
  rm -r /tmp/smssmtptemp
  rm -r /var/opt/SMSSMTP
  rm -r /opt/Symantec
  rm -f /etc/Symantec.conf
  rm -f /etc/symantec.reg
  rm -f /etc/liveupdate.conf
  rm -f /var/log/SYMANTEC.error
  rm -f /var/log/SMSSMTP-install.log
  These commands are based on default directory locations. If you changed the default directory locations, modify the commands to use the appropriate directories.

Uninstall Symantec Mail Security for SMTP from Windows 2000/2003 Server

There may be files and registry entries that are not removed when you uninstall Symantec Mail Security for SMTP. You must manually delete those files and entries.

Warning: If you are running other Symantec products, certain shared files, including registry files, should not be deleted.

To uninstall Symantec Mail Security for SMTP from Windows

- Do one of the following:
  - In the Windows Control Panel, double-click **Add/Remove Programs**, click **Symantec Mail Security for SMTP 4.1**, and then click **Remove**.
  - From the Start menu, select **Programs** > **SMSSMTP** > **Uninstall Symantec Mail Security for SMTP**.

To manually delete files that are left behind after uninstallation

1. Go to C:\Program Files\Symantec\SMSSMTP.
2. Delete the SMSSMTP folder.
3. In the Add/Remove Programs list, delete Java LiveUpdate.

To manually delete registry entries that are left behind after uninstalling

1. On the Windows taskbar, click **Start** > **Run**.
2. In the Run window, type **regedit**.
3. Click **OK**.
4. In the Registry Editor window, under My Computer, double-click **HKEY_LOCAL_MACHINE**.
5. Double-click **SOFTWARE**.
6. Right-click the Symantec folder, and then click **Delete**.
   Do not delete the folder or any shared files from the folder if you are running other Symantec products.
7. In the Confirm Key Delete window, click **Yes**.

Chapter 3

Configuring Symantec Mail Security for SMTP

This chapter includes the following topics:

Configuring administrator settings

The following types of administrator accounts can be set in Symantec Mail Security for SMTP:

- Administrator: Oversees administration of Symantec Mail Security for SMTP
- Report-only administrator: Has privileges only to run reports on Symantec Mail Security for SMTP

Note: The report-only administrator password must be different from that of the administrator.

Configure administrator settings

Table 3-1 describes the administrator settings that you can configure through the administrative interface.

Table 3-1 Administrator settings

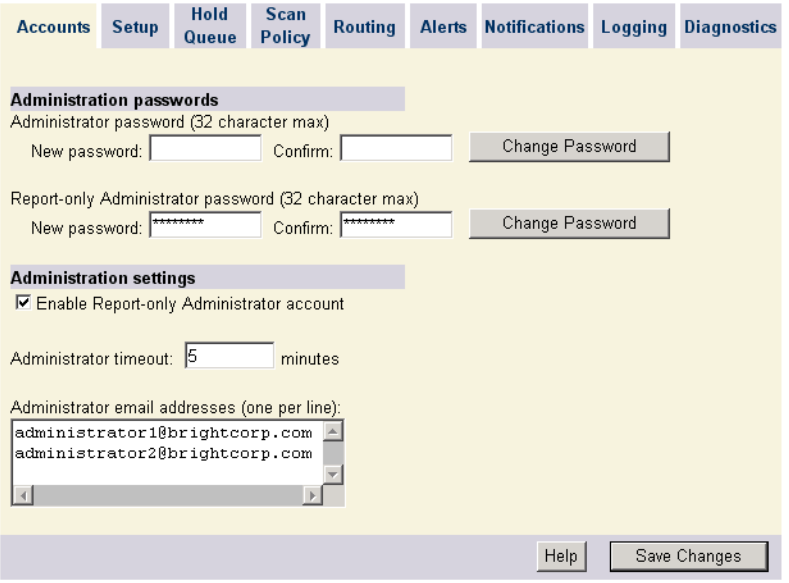
Setting	Description
Administrator password	The administrator password is set during installation and can be changed through the administrative interface.
Report-only administrator password	The report-only administrator password can be set only through the administrative interface.
Administrator timeout	The administrator timeout applies to both the administrator and the report-only administrator accounts.
Administrator email addresses for notifications and alerts	You can specify the addresses to which notifications and alerts are sent when policy violations occur.

To change an administrator password through the administrative interface

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Accounts tab, under Administration Passwords, under Administrator password, in the New password box, type a password for the administrator.
   Passwords are case-sensitive and have a 32-character limit.
   You do not need to set a password through the administrative interface unless you want to change the password that you set during installation.
3. In the Confirm box, type the password again.
4. Click **Change Password**.

To set a report-only administrator password through the administrative interface

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.



2. On the Accounts tab, under Administration Passwords, under Report-only Administrator password, in the New password box, type a password for the report-only administrator. (Ensure that the password is different from that of the Administrator.)
   Passwords are case-sensitive and have a 32-character limit.

3 In the Confirm box, type the password again.

4 Click **Change Password**.

To enable the report-only administrator account

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Accounts tab, under Administration Settings, check **Enable Report-only Administrator account**.

3 Click **Save Changes**.
The report-only administrator password must be set before enabling the account.

To set the administrator timeout

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Accounts tab, under Administration Settings, in the Administrator timeout box, type the number of minutes that should elapse without activity before a new logon is required.
Five minutes is the default.
The administrator timeout applies to both the administrator and the report-only administrator.

3 Click **Save Changes**.

To set administrator email addresses for notifications and alerts

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Accounts tab, under Administration Settings, in the Administrator email addresses box, type the email addresses to which notifications and alerts will be sent.
Type one email address per line.

3 Click **Save Changes**.
In addition to setting an email address for notifications and alerts, you must configure Symantec Mail Security for SMTP correctly to have it send notifications and alerts. This is done through the Notifications and Alerts tabs.

Configuring connection and delivery options

You may configure the following in Symantec Mail Security for SMTP:

- SMTP connection
  See "Configuring SMTP options" on page 49.
- Delivery options
  See "Configuring delivery options" on page 51.
- HTTP connection
  See "Configuring HTTP connections" on page 52.
- HTTPS connection
  See "Configuring HTTPS options" on page 53.
- Custom disclaimer
  See "Configuring a custom disclaimer" on page 55.
- Local time zone
  See "Configuring the local time zone" on page 56.
- Temporary directory location
  See "Changing the temporary files directory location" on page 56.

Configuring SMTP options

The port numbers for SMTP, HTTP, or HTTPS must be unique. To change more than one port number to a port number that is used by another application, you must change one port number at a time. If you change more than one port number at a time, and you switch, for example, the port number that is used for HTTP with the port number that is used for HTTPS, you will receive an error message because Symantec Mail Security for SMTP recognizes those port numbers as already being in use.

SMTP options apply to the Symantec Mail Security for SMTP server, which receives email messages for scanning and then forwards the messages for delivery.

To configure SMTP options

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under SMTP, in the SMTP port number box, type the port number for the port on which Symantec Mail Security for SMTP listens.
   The default is 25.
   If the SMTP port is reset to another port, only email messages that arrive at the other port will be processed. If a port number is entered that is already used, the SMTP port number reverts to the previously assigned port number and a warning message is displayed.
3. In the Maximum number of outgoing connections drop-down list, select the number of simultaneous connections for outgoing email.
   The default is 30. Increasing the default augments the resources that are required by the program and diminishes performance. Unless you have a compelling reason to do otherwise, accept the default.
   Additional connections are queued when the system is already processing the maximum number of connections that are allowed.
   Multiprocessor computers can effectively use more connections than single processors.
4. On the Maximum number of incoming connections menu, select the number of simultaneous connections for incoming email.
   The default is 15. Unless you have a compelling reason to do otherwise, accept the default.
   Setting the number of connections too high can slow processing. Additional connections are queued when the system is already processing the maximum number allowed.
5. In the Alert/Notification “From:” box, type the text that you want to appear in the From field when Symantec Mail Security for SMTP notifications are sent.
   The default is Symantec_Mail Security_for_SMTP.
   The From field accepts one user name or fully qualified domain address, which means that the From field can be set to a real account. In this case, recipients of Symantec Mail Security for SMTP-generated messages, alerts, and notifications can reply to that account.
6. Click **Save Changes**.

Configuring delivery options

During a virus outbreak, you may want to pause delivery of messages or reject incoming messages. You can also specify the number of days to attempt to deliver messages that cannot be delivered on the first attempt.

Configure delivery options

Follow these instructions to pause delivery, reject incoming messages, and set the number of days to attempt message delivery.

To pause delivery of messages

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under Delivery, check **Pause message delivery**.
   While this is checked, messages are still received and placed in the fast queue, but no messages are delivered. Once it is unchecked, the stored messages are processed as usual.
3. Click **Save Changes**.

To reject incoming messages

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under Delivery, check **Reject incoming messages**.
   While this is checked, no incoming messages are accepted, and the sending server receives notification that the service is not available. Once it is unchecked, incoming messages are accepted and processed as usual.
3. Click **Save Changes**.

To set the number of days to attempt message delivery

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under Delivery, in the Number of days drop-down list, select the number of days that Symantec Mail Security for SMTP will attempt to deliver a message.
   If a message cannot be delivered, it is sent to the slow queue where Symantec Mail Security for SMTP continues to attempt delivery. If a message cannot be delivered after the set number of days, it is returned to the sender and deleted from the slow queue and from the system.
3. Click **Save Changes**.

Configuring HTTP connections

The Symantec Mail Security for SMTP software is managed through a Web-based interface. This interface is provided through a built-in Hypertext Transfer Protocol (HTTP) server that is included with the software. This HTTP server is independent of any existing HTTP server that is already installed on your server and is not a general-purpose Web server.

The HTTP port number is set during installation, but it can be changed through the administrative interface.

To configure HTTP connections

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under HTTP/HTTPS, in the HTTP port number box, type the port number on which the built-in HTTP server will listen.
   The number that you specify becomes the port number in the URLs that you use to access the Symantec Mail Security for SMTP administrative interface. The port number must be exclusive to Symantec Mail Security for SMTP and must not already be in use by any other program or service.
   Because the built-in HTTP server is not a general purpose Web server, do not use port number 80 (the default port number for general-purpose Web servers). You should use the default port number of 8003. If you select a port number other than the default, remember which port number you selected.
3. Click **Save Changes**.

Configuring HTTPS options

During installation, you must identify the port number for your HTTPS server. You can define an HTTPS server connection between computers on your network and Symantec Mail Security for SMTP to encrypt passwords during logon sessions and password changes using SSL encryption.

Note: You must have an SSL Web server certificate installed before you enable SSL encryption for logons.

Configure HTTPS options

You must do the following to configure HTTPS options:

- Generate an SSL certificate request.
- Submit the certificate request to a recognized Certificate Authority.
- Install the certificate that is returned from the Certificate Authority.
- Enable SSL encryption.

To generate an SSL certificate request

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, in the HTTPS port number box, type the port number of the HTTPS server.
   The default port number is 8043. The port number must be exclusive to Symantec Mail Security for SMTP and must not already be in use by any other program or service.
3. Click **Certificate Management**.
4. In the Certificate Management window, under Request, in the Common Name box, type the IP address or resolvable host name of the computer that is running Symantec Mail Security for SMTP (for example, smart.brightschool.com).
   Check the Web site of the Certificate Authority to which the request will be submitted to see if there are format restrictions. For example, some Certificate Authorities require a resolvable host name instead of an IP address. Some require that the state or province name be spelled out.
5. In the Organization box, type your organization's name (for example, Bright School).
6. In the Organization Unit box, type your business's main function (for example, Education).

7 In the City/Locality box, type your city or locality.

8 In the State/Province box, type your state or province.
If you do not have a state or province, you must type something in this field.

9 In the Country/Region drop-down list, select your country or region.

10 In the E-mail Address box, type your email address.
The certificate will be sent to the email address that is typed in this box.

11 Click **Create Request**.
The certificate request is displayed in the Certificate Management Request window.

To submit the certificate request to a recognized Certificate Authority

1 In the Certificate Management Request window, copy the entire request, including the header and footer, to your clipboard or to a text file.

2 Click **OK**.

3 Submit the clipboard contents or the copied text file to a recognized Certificate Authority (for example, VeriSign®) by pasting it on the Certificate Authority's site, as they direct.
The Certificate Authority sends your certificate by email to the address that you typed on the Certificate Request page.

To install the returned certificate on Symantec Mail Security for SMTP

1 Copy the entire certificate, including the header and footer, that you received from the Certificate Authority.

2 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.

3 On the Setup tab, under HTTP/HTTPS, click **Certificate Management**.

4 In the Certificate Management window, under Install, paste the copied certificate, including the header and footer.

5 Click **Install Certificate**.

To enable SSL encryption

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under HTTP/HTTPS, check **Enable SSL & encryption for logons**.
3. Click **Save Changes**.
   In the Certificate Management window, under Status, the following information should appear:
   - Date on which the private key was installed
     This was done automatically when you generated your request.
   - Date on which the certificate was installed
   - Date on which the certificate expires
     Expiration information is displayed only when SSL is enabled.

Acting as your own Certificate Authority

If you are able to act as your own Certificate Authority, you need only install a signed certificate that is created from the request that is generated by Symantec Mail Security for SMTP and enable SSL encryption for logons.

See "To install the returned certificate on Symantec Mail Security for SMTP" on page 54.

See "To enable SSL encryption" on page 55.

Configuring a custom disclaimer

You can include text (up to 1000 characters) in every scanned message that is not destined to domains in the local routing list. You should use only ASCII characters to ensure proper display. Other characters, such as DBCS, may not display properly.

To configure a custom disclaimer

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under Custom disclaimer, check **Enter text to be included in every scanned message**.
3. In the text box, type your message.
4. Click **Save Changes**.

Configuring the local time zone

You can change the local time zone region that is used to format the date and time for logging and reporting purposes. If the selected time zone does not match the local time zone of the server, all report times will be offset to the server local time.

To configure the local time zone

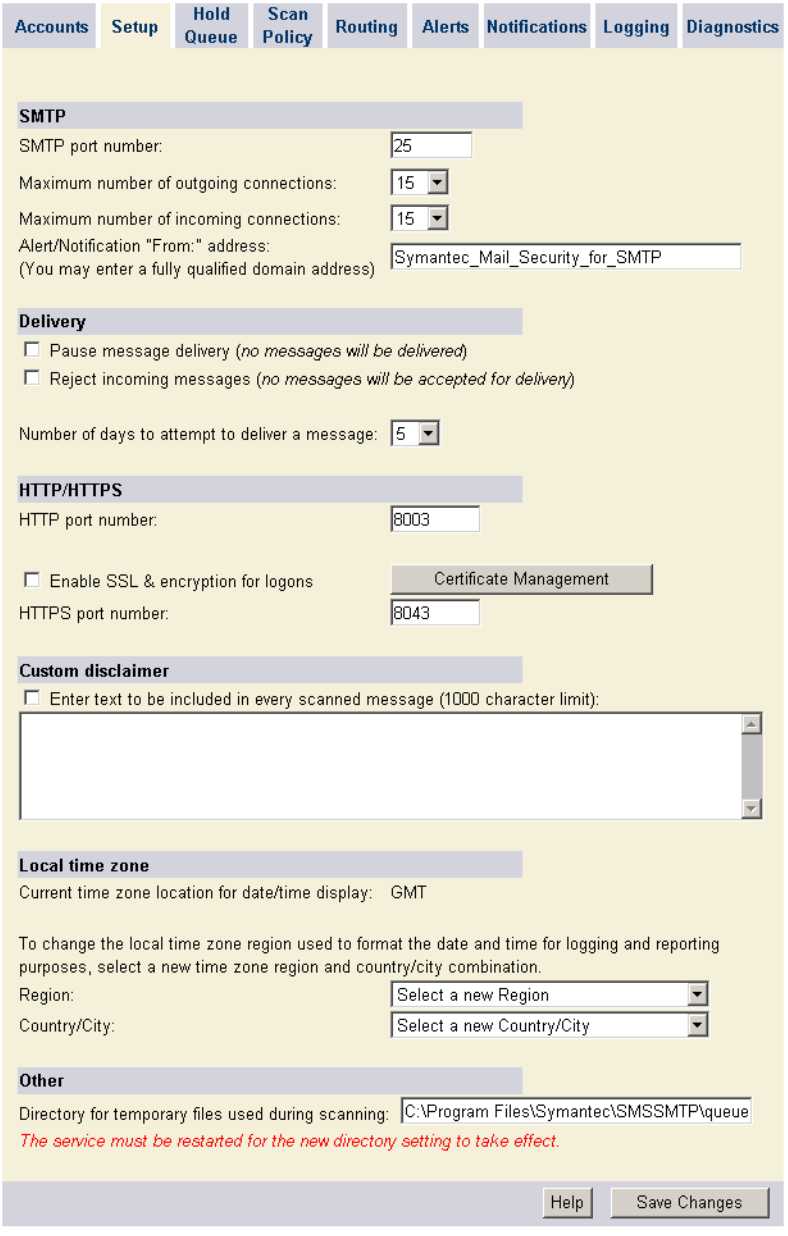
1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under Local time zone, in the Region drop-down list, select a region.
3. On the Country/City drop-down list, select a country or city.
4. Click **Save Changes**.

Changing the temporary files directory location

During installation, you select the locations for all directories. Through the administrative interface, you can change the location for the directories that contain temporary files that are created during Symantec Mail Security for SMTP scanning.

To change the temporary files directory location

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.



2 On the Setup tab, under Other, in the Directory for temporary files used during scanning box, type the directory path where temporary files will be stored during scanning.
The Windows default is \Program Files\Symantec\SMSSMTP\queues\Temp
The Solaris default is /tmp/smssmtptemp
When a nondefault directory is set, a subdirectory named SMSSMTP is created in the nondefault location.

3 Click **Save Changes**.
The service must be restarted for the new directory setting to take effect.

Processing messages in the hold queue

Messages are placed in the hold queue in one of the following ways:

- If a message causes a system crash three times, it is moved to the hold queue.
- If Symantec Mail Security for SMTP is configured to hold messages that cannot be processed, those messages are sent to the hold queue.
See "Configuring scan options" on page 60.

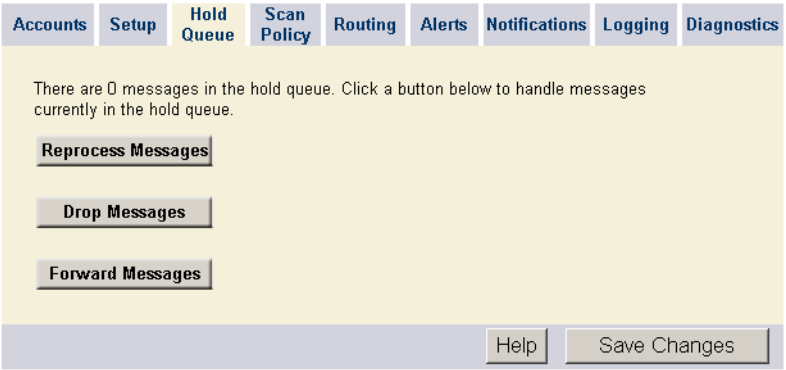
Process messages in the hold queue

You can configure Symantec Mail Security for SMTP to reprocess, drop, or forward a copy of messages in the hold queue.

Warning: Reprocessing messages is not recommended. Reprocessing a message that has caused a system crash will likely result in another system crash.

To reprocess messages that are in the hold queue

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.



2 On the Hold Queue tab, click **Reprocess Messages**.

3 In the Reprocessing Hold Queue Messages window, click **Yes**.
All messages that are in the hold queue are reprocessed.

To drop messages that are in the hold queue

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Hold Queue tab, click **Drop Messages**.

3 In the Dropping Hold Queue Messages window, click **Yes**.
All messages that are in the hold queue are dropped from your system and are not delivered.

To forward messages that are in the hold queue

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Hold Queue tab, click **Forward Messages**.

3 In the Forwarding Hold Queue Messages window, click **Yes**.

4 In the Subject box, type the subject for the forwarded email messages.

5 In the Email address box, type one email address to which email messages in the hold queue are to be forwarded.

6 Click **Forward**.
Copies of messages in the hold queue are forwarded. Copies are not scanned. Originals remain in the hold queue until they are dropped.

Configuring scan options

Part of setting your antivirus policy is setting a scan policy (determining what types of files are to be scanned and how to handle files that cannot be processed). By default, all files are scanned regardless of extension. For maximum security, do not change the default setting.

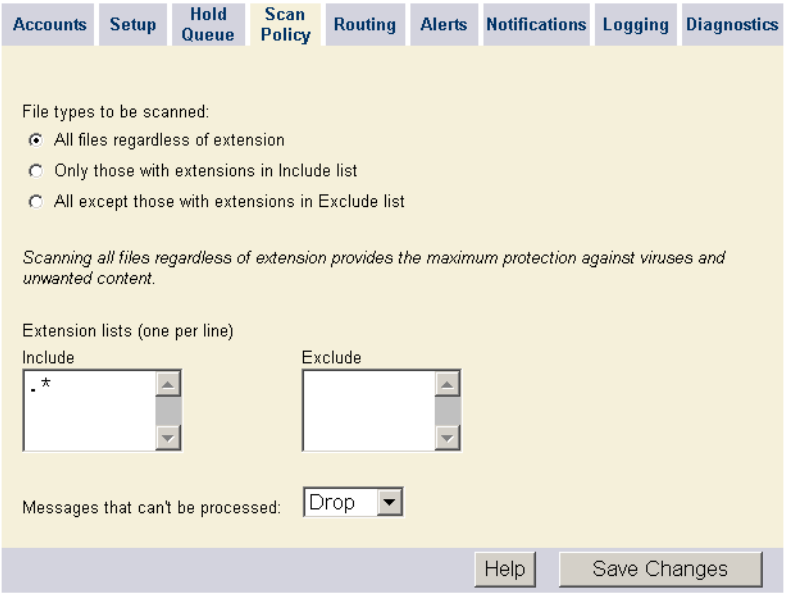
However, processing efficiency may be increased by identifying specific file types to scan. You can specify in the Include list those file types that are commonly at risk of infection. If the Include list includes .zip and .exe but not .cmd, and a container file, for example, test.zip, contains test.exe and test.cmd, only test.exe is scanned.

The Exclude list can be used to identify file types that are unlikely to carry viruses, for example, .gif, .jpeg, or .jpg.

All container files in the Exclude list are decomposed, and the files within them are scanned for viruses. For example, if test.zip contains test.exe and test.doc, and .zip is in the Exclude list, the .exe and .doc files are scanned and repaired or deleted because they did not match the .zip entry. If only .zip is in the Include list and test.zip is sent, no files are scanned because the zip file has been decomposed, and Symantec Mail Security is looking for .zip files.

To configure scan options

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration.**



2 On the Scan Policy tab, select one of the following:

- All files regardless of extension
- Only those with extensions in Include list
- All except those with extensions in Exclude list

3 If Only those with extensions in Include list or All except those with extensions in Exclude list is selected, in the appropriate box, type one extension per line using the following format:

.ttt

Extensions must be preceded by a period (.). Extensions are not case-sensitive.

4 In the Messages that can't be processed drop-down list, select one of the following:
   - Deliver
   - Drop
     You should drop messages that cannot be processed due to scan errors. Most messages that cannot be processed have malformed MIME formatting or corrupted content that cannot be expanded for scanning.
   - Hold
5 Click **Save Changes**.

Configuring routing options

After it scans for viruses, Symantec Mail Security for SMTP routes email messages to your existing hosts for delivery. The routing configurations are as follows:

- Default routing
  See "Configuring default routing" on page 62.
- Local routing
  See "Configuring local routing" on page 64.

Configuring default routing

Setting default routing is not required in most environments but must be done if no local routing is set.

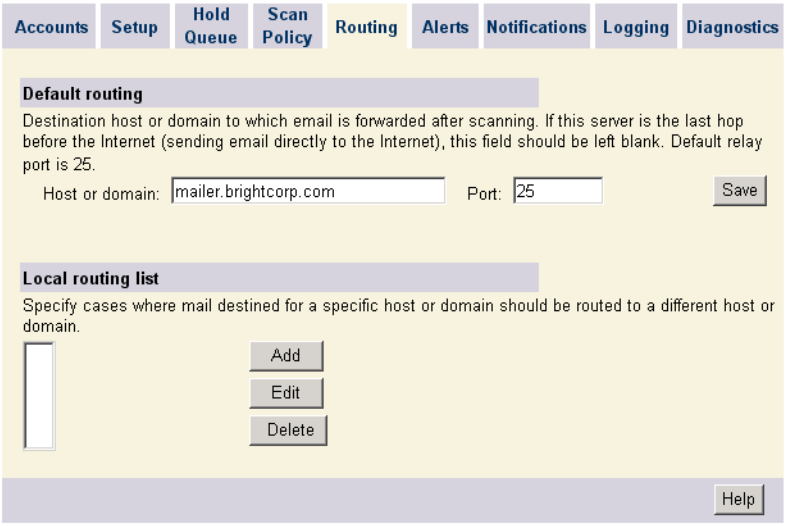
See "Preventing relaying" on page 135.

If the Default Routing box is filled in, any email message that is not addressed to a host or domain in the Local Routing list (a name by itself or the name on the left side of an arrow) is forwarded to the server on your network that is listed in the Default Routing box.

If this box is not filled in, any email message that is not addressed to a name in the Local Routing list is delivered to the appropriate SMTP server on the Internet.

To configure default routing

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.



2 On the Routing tab, under Default Routing, in the Host box, type the fully qualified host name or IP address of your mail server.

3 In the Port box, type the port number of your mail server.
The default port number is 25.

4 Click **Save**.
Mail that was destined for your SMTP server goes to Symantec Mail Security for SMTP for processing and then is forwarded to the specified SMTP server for delivery.

Configuring local routing

Note: You must set a routing list entry for each email domain on your network with the domain (for example, brightcorp.com) as the Routed host or domain and your mail server as the Destination relay.

Setting local routing is required in most environments and is essential if you are not using default routing. The typical setting for most environments is an email domain routed to an SMTP server.

The local routing list has the following purposes:

- It defines special rules for relaying scanned email messages.
- It identifies which domains and hosts are considered local.

The types of local routing entries are as follows:

- An entry (host name, domain, or IP address) by itself
  An entry by itself means that Symantec Mail Security for SMTP treats email messages that are addressed to that host name, domain, or IP address as local. It does a DNS lookup for the address and delivers it to the address that is specified in the MX record.
- An entry (host name, domain, or IP address) followed by another entry
  An entry followed by another entry means that when Symantec Mail Security for SMTP receives and processes email messages that are addressed to the host name, IP address, or domain of the first mail server, it should use the second entry to relay the mail.
  For example, if you type brightcorp.com in the Routed host or domain box and mailer.brightcorp.com in the Destination relay box, after Symantec Mail Security for SMTP processes email messages that are addressed to brightcorp.com (user@brightcorp.com), it forwards the email message to mailer.brightcorp.com for delivery.

In both cases, the first (or only) entry is considered local. The second entry (if any) is not. Local routing rules always have priority over the Default Routing setting.

Designating a host as local is significant for the relay restrictions.

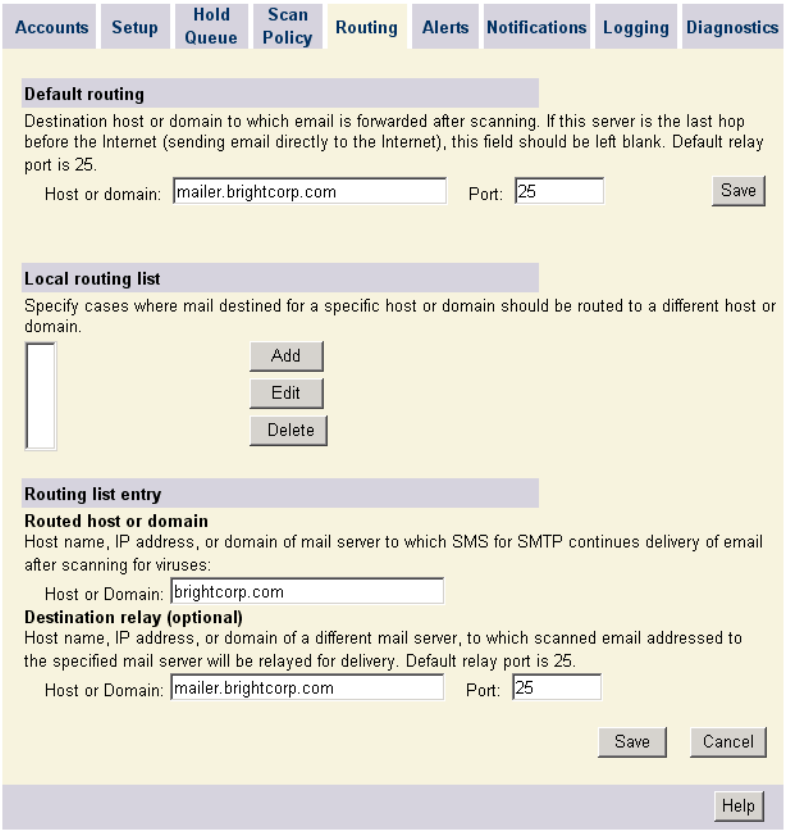
See “Preventing relaying” on page 135.

Configure local routing

You can create, edit, and delete local routing list entries.

To create local routing entries

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.



2 On the Routing tab, under Local Routing List, click **Add**.

3 Under Routing list entry, type the host name, IP address, or domain of a mail server to which email should be routed.

Wildcard characters may be used in routing list entries.

If you type only the first entry and no destination relay, email that is addressed to a user who receives mail at that host will be relayed using that host.

4 Under Destination relay, in the Host box, type the host name, IP address, or domain of the mail server to which email that is destined for the server that is designated under Routed host or domain should be routed.
In most cases, using an IP address is preferable to using a host name because a host name needs to be resolved.
If you type a destination host, email that is addressed to a user who is receiving mail at the host that is listed under Routed host or domain will be relayed using the host that is designated in the Host box under Destination relay.

5 In the Port box, type the port number for the mail server.
The default port number is 25.

6 Click **Save**.

To edit a local routing list entry

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Routing tab, under Local Routing List, select the case that you want to edit.

3 Click **Edit**.

4 Make the changes that you want.

5 Click **Save**.

To delete a local routing list entry

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Routing tab, under Local Routing List, select the case you want to delete.

3 Click **Delete**.

Configuring alerts

You can configure Symantec Mail Security for SMTP to send alerts for system events to one or more administrators.

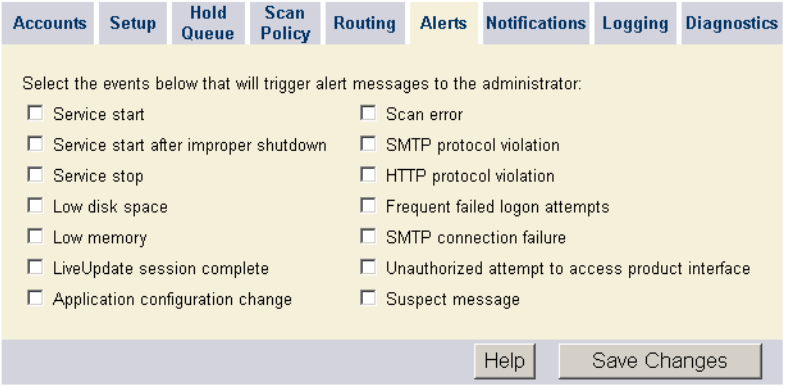
If you do not provide an administrator email address, Symantec Mail Security for SMTP prompts you to save any changes. Alerts will not be delivered, despite being enabled, until an address is specified

See "To set administrator email addresses for notifications and alerts" on page 48.

Note: Sending alerts increases the load of the server. On a heavily used mail server, you should limit the number of alerts that you enable.

To configure alerts

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.



2 On the Alerts tab, select the events that will trigger alerts to the administrator.

The alerts will be sent to the email addresses that you designated when you configured the administrative settings.

3 Click **Save Changes**.

Table 3-2 lists the system events that trigger alerts, their descriptions, and examples of alerts.

Table 3-2 Events that trigger alerts

Event	Description	Alert text
ServiceStart	The service has started.	Subject: Service Start Body: The service has been started.
Service start after improper shutdown	The service has started after a shutdown that did not allow services to run normal shutdown scripts (for example, a forced reboot of the server).	Subject: Service Start After Improper Shutdown Body: The service has been started after an improper shutdown.
Service stop	The service has stopped.	Subject: Service Stop Body: The service has been stopped.
Low disk space	The disk space in the logging, email scanning, or mail queuing directory is less than 10 percent.	Subject: Low Disk Space Threshold Exceeded Body: The [ ] directory is running dangerously low on disk space, where [ ] is either logging, email, or mail queuing.
Low memory	Less than 10 percent of memory remains.	Subject: Low Memory Threshold Exceeded Body: The memory available on the server is running dangerously low.
LiveUpdate session complete	LiveUpdate has successfully completed a virus definitions update.	Subject: LiveUpdate Completed Body: The system completed a LiveUpdate operation.
Application configuration change	The software has been reconfigured in some way.	Subject: Configuration Change Body: A configuration change was made.

Table 3-2 Events that trigger alerts

Event	Description	Alert text
Scan error	The engine that handles decomposition of files has encountered an error during scanning. Encrypted containers are not considered scan errors. They are handled separately based on product configuration.	Subject: Decomposition error Body: An error occurred during message decomposition.
SMTP protocol violation	During communication, a protocol violation between SMTP servers has been detected.	Subject: SMTP Protocol Violation Body: An SMTP protocol violation was detected by the server.
HTTP protocol violation	During communication, a protocol violation with the HTTP server has been detected.	Subject: HTTP Protocol Violation Body: An HTTP protocol violation was detected by the server.
Frequent failed logon attempts	Three unsuccessful logon attempts have been made. An alert is sent on the third attempt, and one is sent for every unsuccessful attempt thereafter. The counter is reset upon correct logon.	Subject: Frequent Failed Logon Attempts Body: Several failed logon attempts have been made to the server.
SMTP connection failure	The SMTP server that Symantec Mail Security for SMTP is trying to contact is not available.	Subject: SMTP Connection Failure Body: A connection failure was encountered by the server.
Unauthorized attempt to access product interface	Users, including Report-only administrators, have attempted to access the administrative interface without appropriate permissions.	Subject: Unauthorized Attempt to Access Product Interface Body: An unauthorized attempt to access the server interface was detected.

Table 3-2 Events that trigger alerts

Event	Description	Alert text
Suspect message	On the third attempt to send a message that crashes Symantec Mail Security for SMTP or a message that triggers a “Cannot Scan” error, the message is considered suspect and moved to the hold queue.	Subject: Suspect Message Body: A suspect message was received by the server.

Configuring notifications

You can configure Symantec Mail Security for SMTP to send notifications to administrators and senders when antivirus and blocking policies have been violated.

If you do not enter an administrator email address, Symantec Mail Security for SMTP prompts you to enter one each time the Notifications screen is saved. Administrator notifications will not be delivered, despite being enabled, until an address is specified.

See “To set administrator email addresses for notifications and alerts” on page 48.

Understanding notifications

Violation notifications have the following text:

- Subject: SMSSMTP Policy Violation
- Message: The following message sent by this account has violated system policy:
  $ {MSGINFO}
  The following violations were detected:
  $ { VIRUSINFO}
  $ {CONTENTINFO}
  $ {ENCRYPTINFO}

Administrator notifications have the additional metatag $ {DISPOSITION} at the end of the message.

Understanding notification metatags

Within the default text of notifications, there are metatags, which act as placeholders for information. You can change text in any notification, but do not alter the metatags, or you will not receive information about the event that triggered the notification.

Table 3-3 describes all available metatags and shows examples.

Table 3-3 Notification metatags

Metatag	Description	Example
MSGINFO	Tag in Policy Violation notification to sender and administrator. Contains From/To information.	■ From: somebody@domain.com ■ To: someone@domain.com
DISPOSITION	Tag in Policy Violation notification to administrator. Contains information about how the message was handled.	The message was dropped
CONTENTINFO	Tag in Policy Violation notification to administrator and sender. Contains content filter-specific data for the following: ■ Subject line blocked ■ Container limit exceeded ■ File name blocked	■ Subject: <specified by user> Matching Subject: <subject line matched> ■ The extracted attachment depth exceeded set limits. ■ File: <list of blocked file names> Matching file name: <file name matched>
VIRUSINFO	Tag in Policy Violation notification to sender and administrator. Contains virus-specific data, such as virus name and signature number.	Virus scan results follow <list of specific virus information>
ENCRYPTINFO	Contains information about encrypted container detection.	Message contained an encrypted container

Configuring notifications

You can configure Symantec Mail Security for SMTP to send administrator and sender notifications when the following is detected:

- Infected file
- Outbreak alert
- Content violation
- Container limit violation
- Encrypted container

Note: Notifications are not sent for antispam, content, or spam rule violations.

To configure notifications

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Notifications tab, under Violation notifications, select Administrator, Sender, or both.
3. If you selected to notify the administrator, under Message for administrator, either accept the default Subject and Body text or delete the default text and type your own.
4. If you selected to notify the sender, under Message for sender, either accept the default Subject and Body text or delete the default text and type your own.
5. Click **Save Changes**.
   Do not alter the metatags ({$MSGINFO}, for example). Metatags act as placeholders for information that will be included in notifications.

Configuring logging options

Symantec Mail Security for SMTP lets you send logging events to the local computer or to SESA. Local logging (logging of activity to the computer on which Symantec Mail Security for SMTP is running) is enabled by default. For local logging, you can specify how long old logs should be retained, from one week to never delete.

SESA logging (logging of activity to the SESA Console) is not enabled by default.

See "To configure logging options" on page 73.

See "Integrating Symantec Mail Security for SMTP with SESA" on page 155.

Once enabled, Symantec Mail Security for SMTP logs the following local events to SESA:

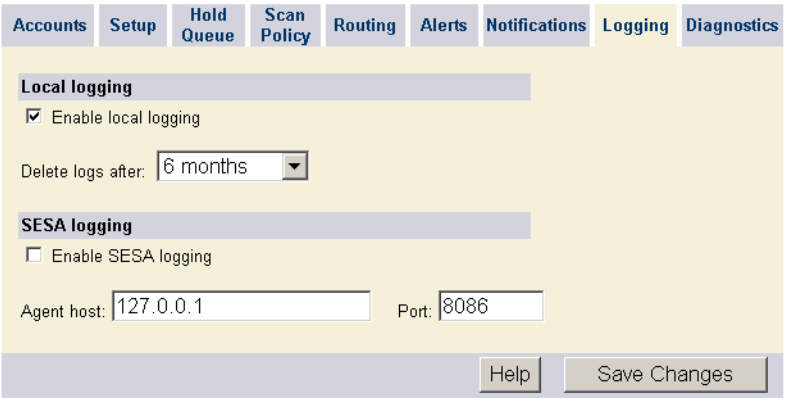
- Logon
- Logoff
- Definitions updated
- Object modified
- Protocol violation
- Messages rejected
- Messages dropped
- Messages bounced
- Delivery failed
- Virus logged
- Files repaired
- Files deleted
- Subjects blocked
- Scan error
- Sender blocked
- Attachment deleted
- Spam list block
- Heuristic spam detection
- Message statistics
- Spam rule violations
- Content rule violations
- Messages held
- Encrypted content violations

See "Generating detail reports" on page 148.

No data is retained while logging is disabled, so you cannot generate reports unless logging is enabled.

To configure logging options

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.



2 On the Logging tab, under Local logging, check or uncheck **Enable local logging**.

3 In the Delete logs after drop-down list, select the time period to retain log files.

4 Under SESA logging, check or uncheck **Enable SESA logging**.

5 In the Agent host box, type the IP address on which the SESA agent listens.

6 In the Port box, type the port number on which the SESA agent listens.

7 Click **Save Changes**.

Configuring queue file save and SMTP conversation logging

Diagnostic files are located on Windows and Solaris in the queues/diagnostic files directory. If you contact Symantec Technical Support for assistance, you may be instructed to configure the Queue File Save or conversation logging setting.

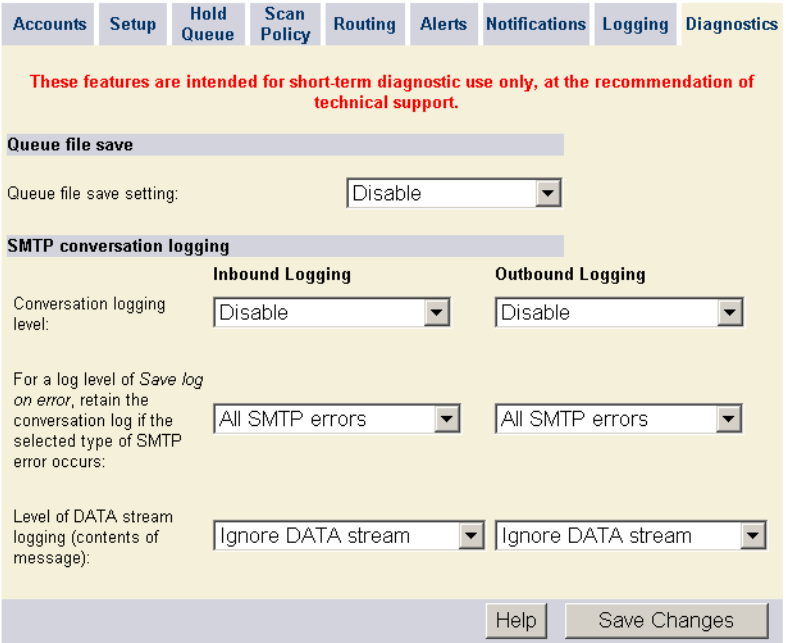
Warning: The default for the Queue File Save setting is Disable. Do not change this setting unless you are instructed by Symantec Technical Support to do so. Changing the setting can result in undesirable system behavior.

To configure queue file save

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Diagnostics tab, under Queue File Save, in the Queue File Save setting drop-down list, select the setting that Symantec Technical Support tells you to select.

3 Click **Save Changes**.



Configure SMTP conversation logging

You can configure SMTP protocol conversation logging (logs the incoming or outgoing SMTP protocol conversation when accepting or delivering a message). If inbound logging is enabled, one conversation log is generated for each inbound connection. If outbound logging is enabled, one log is generated for each message delivery attempt.

The conversation log files are saved to the diagnostic files directory that is defined during installation. The default location is <InstallDir>/queues/diagnosticfiles, where <InstallDir> is the path of the top-level installation directory, such as var/opt/SMSSMTP or C:\Program Files\Symantec\SMSSMTP.

Warning: SMTP Conversation Logging is disabled by default. Do not change this setting unless you are instructed by Symantec Technical Support to do so.

To configure conversation logging

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Diagnostics tab, under SMTP Conversation Logging, in the logging drop-down lists, select one of the following for the conversation logging level:
   - Disable: No conversation logging is performed.
   - Save log on error: Conversation logs are saved only if an SMTP error occurs during the message transmission.
   - Log all inbound (or outbound) traffic: All conversation logs are saved for inbound or outbound conversations.
3. On the Diagnostics tab, under SMTP Conversation Logging, in the logging drop-down lists, select one of the following to determine error type triggers:
   - All SMTP errors: All SMTP errors are logged.
   - Communication error: Network and socket errors are logged.
   - Protocol error: Failures to follow defined SMTP protocols (such as a command out of sequence or bad syntax) are logged.
   - Local processing error: Application-defined errors (such as a message that exceeds defined size limits) are logged.
   - Unsupported operation: Requests for unsupported operations (such as TURN) are logged.
4. On the Diagnostics tab, under SMTP Conversation Logging, in the logging drop-down lists, select one of the following to determine the level of DATA stream logging:
   - Ignore DATA stream: Only the DATA command is logged.
   - Summarize DATA stream: A line count and byte count summary of the DATA stream is logged.
   - Echo DATA stream: The entire DATA stream is logged.
     For outbound messages, the DATA stream is buffered. (The line count and byte count of the DATA stream for outbound messages will not match the line count and byte count for inbound messages.)

Chapter 4

Setting your antivirus policy

This chapter includes the following topics:

About your antivirus policy

Your antivirus policy is determined by how you configure Symantec Mail Security for SMTP to handle email (which file types to scan, which files to quarantine, and when to notify administrators and senders if viruses are found or virus outbreaks occur).

Configuring antivirus settings

The antivirus settings in Symantec Mail Security for SMTP let you do the following:

- Scan for viruses
  See "Enabling virus scanning" on page 78.
- Handle infected files
  See "Handling infected files" on page 80.
- Clean up mass-mailer messages
  See "Enabling mass mailer cleanup" on page 81.
- Quarantine files
  See "Forwarding infected files to the Central Quarantine" on page 82.

Enabling virus scanning

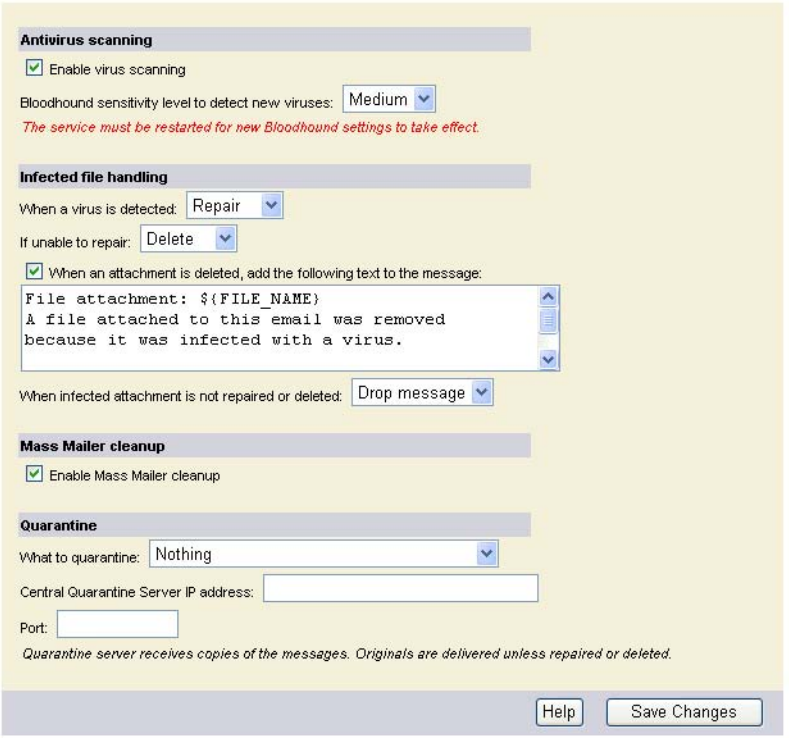
You must enable virus scanning and set the Bloodhound™ sensitivity level through the administrative interface. Bloodhound is the technology Symantec uses to heuristically detect new and unknown viruses.

Note: For information about the latest virus threats and other information about viruses, visit the Symantec Security Response Web site at http:\\securityresponse.symantec.com

---

To enable virus scanning

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Antivirus Policy**.



2 In the Antivirus Settings window, under Antivirus scanning, ensure that Enable virus scanning is checked.

3 In the Bloodhound sensitivity level to detect new viruses drop-down list, select one of the following:
- Off
- Low
- Medium
- High

Medium is the default setting. If you set the Bloodhound sensitivity level to High, resource demand increases, performance may decrease, and occasional false positive detections may be generated.

4 Click **Save Changes**.
Symantec Mail Security for SMTP must be stopped and restarted for Bloodhound changes to take effect.

Handling infected files

Symantec Mail Security for SMTP can handle infected files in a number of ways.

Scanning must be enabled and files must be specified for scanning in order for files to be processed.

See "Enabling virus scanning" on page 78.

See "Configuring scan options" on page 60.

To handle infected files

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Antivirus Policy**.

2 In the Antivirus Settings window, under Infected file handling, in the When a virus is detected drop-down list, select one of the following:
- Repair: An attempt is made to repair the virus, and, if successful, the message is delivered.
- Delete: The infected file is deleted, and the message is delivered.
- Log only: An incident of the virus is logged, and the message (and the infected file) is delivered.

3 In the If unable to repair drop-down list, select one of the following:
- Delete: The infected file is deleted, and the message is delivered.
- Log only: An incident of the unrepairable virus is logged, and the message (with the unrepairable file) is delivered.

4 If you want to delete infected attachments, check **When an attachment is deleted, add the following text to the message** to add a notification message to the email message.
You can retain the default message text, or modify it.

5 In the When infected attachment is not repaired or deleted drop-down list, select one of the following:
- Drop message: Processing of the message stops, and the message is dropped.
- Log only: An incident of the infection is logged, and the message (and the infected file) is delivered.

6 Click **Save Changes**.

Enabling mass mailer cleanup

You can configure Symantec Mail Security for SMTP to delete mass-mailer, worm-infected messages. These types of messages are spread by mailing themselves to names and addresses in users' address books. This feature causes all email messages that are detected as mass mailer worms to be dropped.

When the mass mailer cleanup function is enabled in the administrative interface, Symantec Mail Security for SMTP searches for a match between virus name patterns and the signatures that are returned by the antivirus scan. The match is made based on the configuration parameter @m (used by Symantec Security Response to name mass mailer viruses). If a match is detected, then the message is dropped.

Even when the mass mailer cleanup function is disabled, messages that have detectable viruses in the outer MIME container (that is, the message itself, not the attachments within it) will be dropped. This is because Symantec Mail Security for SMTP believes that the message is infected in a way that is not repairable and not deletable.

To enable mass mailer cleanup

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Antivirus Policy**.

2 In the Antivirus Settings window, under Mass Mailer cleanup, select **Enable Mass Mailer cleanup**.
This option is enabled by default.

3 Click **Save Changes**.

Forwarding infected files to the Central Quarantine

Symantec Mail Security for SMTP can forward messages that contain infected attachments and files within attachments to a separately installed Central Quarantine server. The Central Quarantine must be installed on a Windows 2000 Server computer. Typically, heuristically detected viruses that cannot be repaired by the current set of virus definitions are forwarded to the Central Quarantine and isolated so that the viruses cannot spread.

A copy of each message that contains a virus is forwarded to the Quarantine server. If more than one virus is found within one message, two copies of the message are forwarded (one containing the first virus, the other with the second).

From the Central Quarantine, these items are submitted to Symantec Security Response for analysis. If a new virus is identified, updated virus definitions are returned using LiveUpdate.

See "Updating virus and spam definitions files" on page 84.

Warning: If you configure Symantec Mail Security for SMTP to forward infected messages to the Central Quarantine, and the Central Quarantine is not running, files accumulate in the quarantine directory and may severely degrade performance.

To establish quarantine settings

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Antivirus Policy**.
2. In the Antivirus Settings window, under Quarantine, on the What to quarantine menu, select one of the following:
   - Nothing
   - Messages containing unrepaired infections
     See "Handling infected files" on page 80.
   - Messages containing any infections
3. In the Central Quarantine Server IP address box, type the IP address of the server that is running the Central Quarantine.
4. In the Port box, type the port number for the Central Quarantine.
5. Click **Save Changes**.

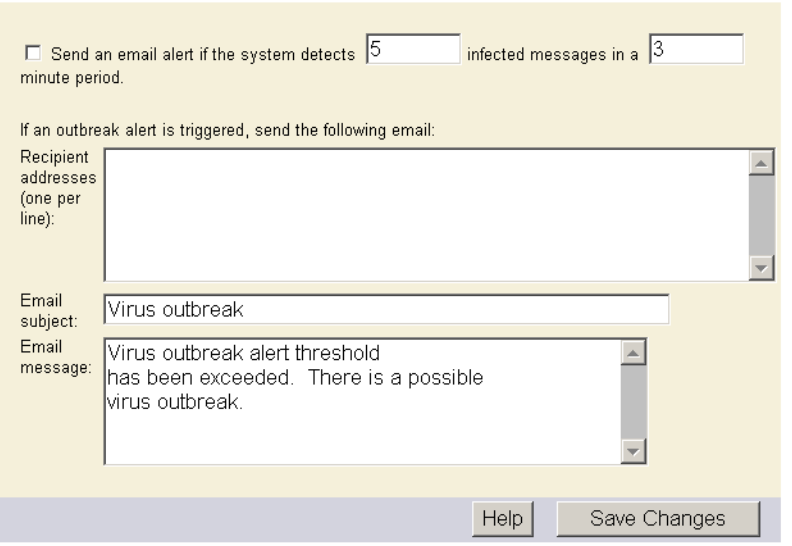
Configuring outbreak alerts

You can configure Symantec Mail Security for SMTP to send notifications to one or more email addresses in cases of virus outbreaks.

Note: You must enter recipient addresses on the Antivirus Policy > Outbreak Alert tab in order for this function to work.

To configure outbreak alerts

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Antivirus Policy**.



2 In the Outbreak Alert window, check **Send an email alert if the system detects [ ] infected messages in a [ ] minute period**.

3 Type in the number of infected messages and the period of time in which those messages must be sent.

4 Type the email addresses (one per line) to which the alert should be sent.

5 If desired, change the default text in the subject and message boxes.

6 Click **Save Changes**.

Updating virus and spam definitions files

Symantec Mail Security for SMTP relies on up-to-date information to detect and eliminate viruses and spam. Symantec supplies updated virus and spam definitions files, which contain information about newly discovered viruses and spam, to ensure that your virus and spam protection is current. Updated virus definitions files are provided at least once per week and whenever a new virus threat is discovered. Spam definitions are updated approximately once per quarter. When new virus definitions files are available, the LiveUpdate technology automatically downloads the proper files and installs them in the proper location.

Spam definitions for Symantec Premium AntiSpam are received through the Symantec Brightmail Logistics and Operations Center (BLOC) and are not updated through LiveUpdate.

Note: To update virus and heuristic spam definitions for Symantec Mail Security for SMTP, you must run LiveUpdate in the product. Running LiveUpdate in other Symantec products will not update your definitions for Symantec Mail Security for SMTP.

For more information on Intelligent Updater, see the Readme file on the Symantec Mail Security for SMTP product CD.

You can configure Symantec Mail Security for SMTP to perform regular updates of virus and spam definitions files using LiveUpdate, or you can set up your own LiveUpdate Server.

See "Setting up your own LiveUpdate server" on page 87.

Update virus and spam definitions files

You can configure Symantec Mail Security for SMTP to run LiveUpdate one or more days per week. You can change the time of day for the first attempt and the frequency of attempts. You can also update virus and spam definitions manually.

To schedule automatic LiveUpdates

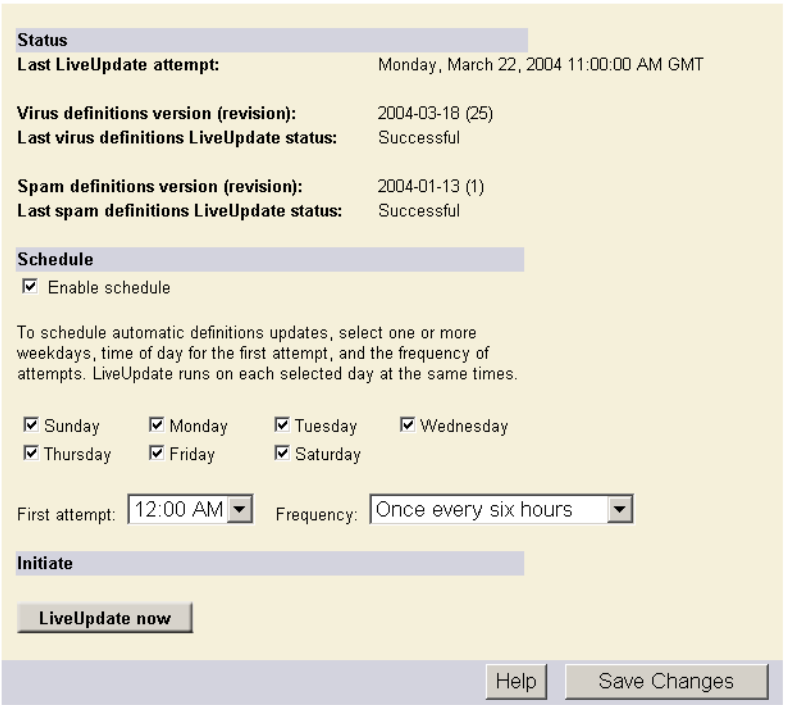
1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **LiveUpdate**.
2. In the LiveUpdate window, under Schedule, check **Enable schedule**. Uncheck this option to disable a scheduled LiveUpdate.
3. Select one or more days on which you want LiveUpdate to run.

4 Select the time of the first attempt and the frequency of attempts.
LiveUpdate runs on each selected day at the same time. For example, selecting Tuesday and Thursday, 06:00 A.M., and Once every four hours, causes LiveUpdate to run only on Tuesdays and Thursdays at 6:00 A.M., 10:00 A.M., 2:00 P.M., 6:00 P.M., and 10:00 P.M. Because LiveUpdate considers midnight the end of the day, it does run for the last time at 10:00 P.M. and does not run again until 6:00 A.M., which is designated as the first attempt.

5 Click **Save Changes**.

To update virus definitions manually

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **LiveUpdate**.



2 In the LiveUpdate window, under Initiate, click **LiveUpdate now**.
Do not resubmit a LiveUpdate request. It may take a few minutes to contact a LiveUpdate server to determine if new updates are available.

Enabling virus definitions updates through Intelligent Updater

By default, Symantec Mail Security for SMTP does not support updating virus definitions through Intelligent Updater. To enable updating through Intelligent Updater, you must run a setup script for your platform. This lets multiple Symantec products that run on the same system share virus definitions updates.

To enable Intelligent Updater for Windows

- Run the following script
  <default directory>\Program Files\Symantec\SMSSMTP\csapi\ AntiVirus\ setup-iu.bat enable
  Symantec Mail Security for SMTP checks shared virus definitions once per minute.

To disable Intelligent Updater for Windows

- Run the following script
  <default directory>\Program Files\Symantec\SMSSMTP\csapi\ AntiVirus\ setup-iu.bat disable
  Symantec Mail Security for SMTP returns to allowing updates through LiveUpdate.

To enable Intelligent Updater for Solaris

- Run the following script
  <default directory>/opt/Symantec/SMSSMTP/csapi/AntiVirus/ setup-iu.sh enable
  Symantec Mail Security for SMTP checks shared virus definitions once per minute.

To disable Intelligent Updater for Solaris

- Run the following script
  <default directory>/opt/Symantec/SMSSMTP/csapi/AntiVirus/ setup-iu.sh disable
  Symantec Mail Security for SMTP returns to allowing updates through LiveUpdate.

Setting up your own LiveUpdate server

The LiveUpdate Administration Utility lets you set up an intranet HTTP, FTP, or LAN server or a directory on a standard file server to handle LiveUpdate operations for your network. The LiveUpdate Administration Utility is provided on the Symantec Mail Security for SMTP product CD.

For more information, see the *LiveUpdate Administrator's Guide* on the Symantec Mail Security for SMTP product CD.

If you set up your own LiveUpdate server, you must edit the LiveUpdate configuration for Symantec Mail Security for SMTP to point to the local LiveUpdate server.

For more information, contact Symantec Service and Support.

Chapter 5

Setting your antispam policy

This chapter includes the following topics:

About antispam policy

Your antispam policy is determined by how you configure Symantec Mail Security for SMTP to handle spam.

Symantec Mail Security for SMTP can handle spam as follows:

Real-time blacklisting	List of mail servers from which mail is rejected
Custom blacklisting	List of sender email addresses and domains that are blocked
Heuristic spam detection	Scan engine that uses an accuracy rating to detect spam
Custom spam rules	Terms that, when found in messages, identify whether a message is spam

You can also create custom and auto-generated whitelists to let Symantec Mail Security for SMTP bypass heuristic and blacklist processing for designated domains and email addresses. (Spam rules still apply.)

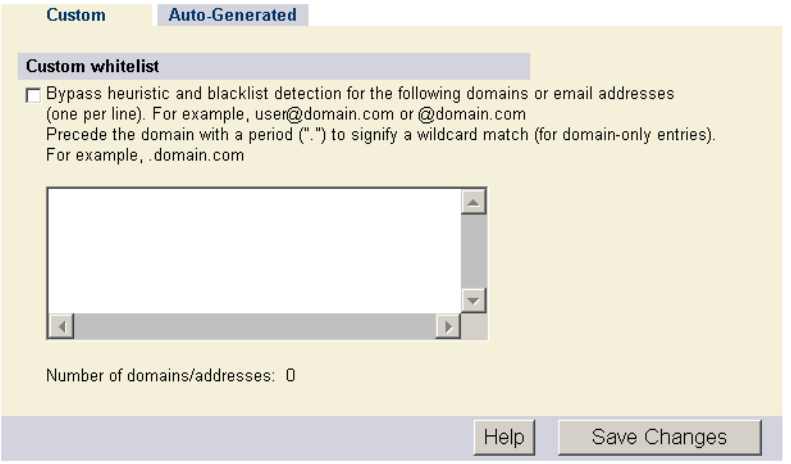
Creating a custom whitelist

You can create a custom whitelist of domains so that email messages from those domains are excluded from all spam processing. If you activate real-time blacklisting and antispam whitelist exclusion, when spam processing begins, Symantec Mail Security for SMTP checks the antispam whitelist first and then queries the real-time blacklists. If the envelope sender matches a domain that is entered in the antispam whitelist, the email message is allowed. If it does not match, real-time blacklists are checked. If there is a match, the email message is blocked.

Email messages from domains that are listed in the whitelist are still processed for content violations (including spam rule violations) and viruses.

To create a custom whitelist

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.



2 In the Whitelist window, on the Custom tab, under Custom whitelist, check **Bypass heuristic and blacklist detection for the following domains or email addresses**.

3 In the exclusion box, type the domains (one per line) to be excluded from regular spam processing.

Domain names must begin with either @ or a period, where a period specifies a wildcard match for any sender at the domain. For example, .company.com would match mail.company.com

You can add fully qualified addresses (for example, user@company.com) to the custom whitelist to exclude email messages from that user from heuristic and blacklist processing.

You must select this option to let the domains bypass spam processing. Spam rule processing still applies.

Activating and managing an auto-generated whitelist

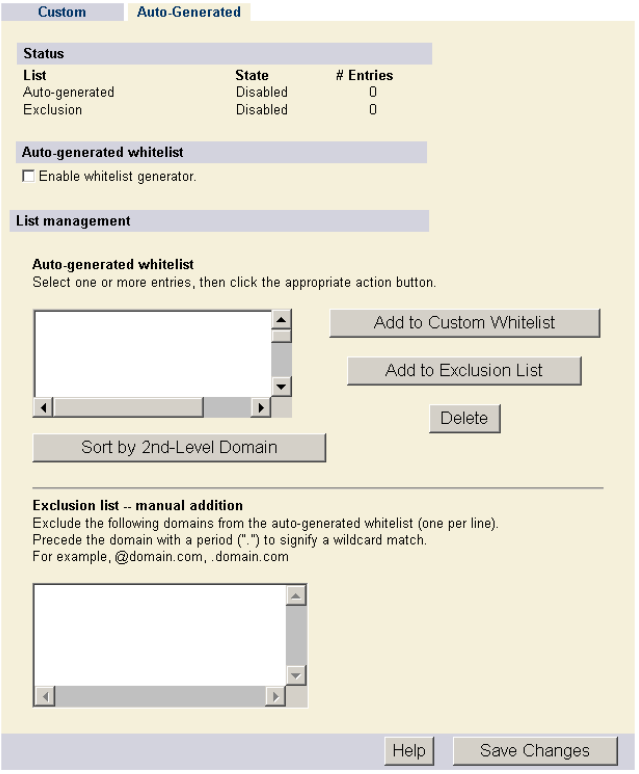
If you activate the auto-generated whitelist feature, the email domains of all outgoing messages that are not in your local routing list are captured in a whitelist. Symantec Mail Security for SMTP stores a maximum of 2000 entries in the auto-generated whitelist. When the maximum number of entries is exceeded, it removes the top 50.

Activate and manage an auto-generated whitelist

You can choose domains from the auto-generated whitelist to add to your custom whitelist, add to your exclusion list, or delete from the list.

To activate an auto-generated whitelist

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.



2 In the Whitelist window, on the Auto Generated tab, under Auto-generated whitelist, check **Enable whitelist generator**.

3 Click **Save Changes**.

To manage auto-generated whitelists

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.

2 In the Whitelist window, under List management, select one or more entries, and then select one of the following actions:

- Add to Custom Whitelist
- Add to Exclusion List
- Delete

3 To sort the list, select one of the following:

Sort by 2nd-Level Domain	When you sort by 2nd-level domain, those domains (for example, something.com) are listed alphabetically based on the root domain. When the root domain is the same but the second-level domain is different, alphabetizing continues using the lower-level domains.
Sort by Frequency	When you sort by frequency, domains from which email is most frequently received appear at the top of the list. A frequency count is listed for each domain.

4 Click **Save Changes**.

To manually add domains to the whitelist

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.

2 In the Whitelist window, on the Auto-Generated tab, under List management, in the Exclusion list box, type the domains (one per line) that you do not want the auto-generated whitelist to track.

Type a period before each domain to signify a wildcard match.

Even if a domain is in the auto-generated whitelist, any additional messages that come from that domain will not increase the frequency count. If a domain that is not in the auto-generated whitelist is added to the exclusion list, messages that are received from that domain are not added to the auto-generated list.

3 Click **Save Changes**.

Blocking by real-time antispam blacklists

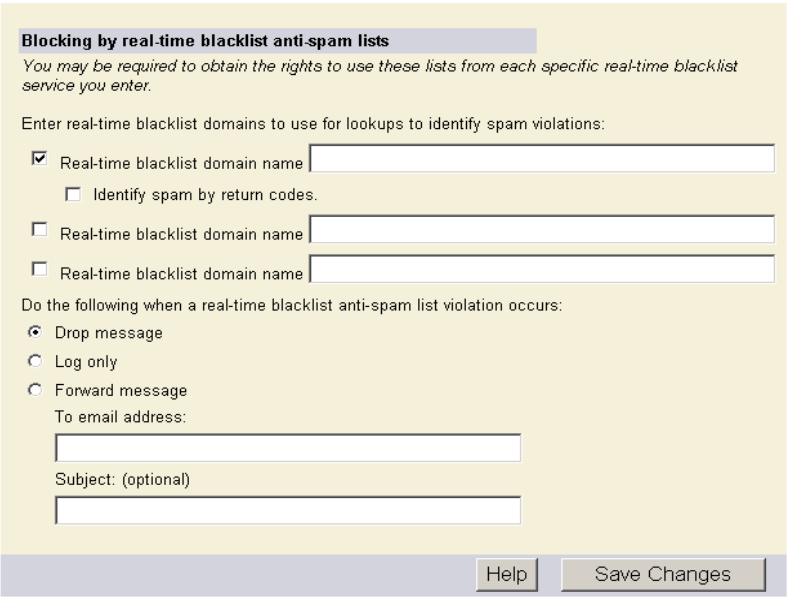
The most common way of preventing spam is to reject mail that comes from mail servers known or believed to send spam. To limit potential spam, Symantec Mail Security for SMTP can support up to three real-time antispam blacklists. Real-time blacklists are DNS-based blocking lists that are generated to limit spam. You may choose to use these lists to drop, forward, or log mail from certain sources, based on criteria that are determined by the list operators. Real-time blacklisting depends on an actively maintained DNS server with a database of IP addresses that are associated with Internet mail servers that are judged to be abusive on one or more spam-related criteria.

Symantec Mail Security for SMTP queries the real-time blacklist for the IP address of a sending mail host. If the query response indicates that the address is listed in the real-time blacklist database, then Symantec Mail Security for SMTP refuses the connection attempt.

Symantec Mail Security for SMTP lets administrators specify up to three domains to query against.

To block by real-time antispam blacklists

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.



2 In the Anti-Spam window, under Real-time Blacklist, check **Real-time blacklist domain name**.

You must check this checkbox to enable this feature. If you do not check this checkbox, Symantec Mail Security for SMTP will not attempt to use this service, even if you type a domain name for the spam service.

3 In the Real-time blacklist domain name box, type the domain of the blacklist service that you will use.

A check box will appear to let you identify spam by return codes. If desired, check the box, and a box will appear to let you type the return codes for identifying email as spam. (Return codes are provided by the blacklist provider if they are necessary.)

4 Type one return code (provided by the blacklist provider) per line to identify email as spam.

Identifying return codes means that only the email messages that are associated with the return codes will be blocked.

If no return codes are listed, any address response from the blacklist is considered as on the list.

To handle antispam list violations

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.

2 In the Real-time Blacklist window, under Blocking by real-time blacklist antispam lists, under Do the following when a real-time blacklist antispam list violation occurs, select one of the following:

- Drop message
- Log only
- Forward message

3 If you selected Forward message, in the To email address box, type one address to which the message will be forwarded, and in the Subject line box, type the subject line to appear for the subject of the forwarded message.

4 Click **Save Changes**.

Blocking by a custom blacklist

You can configure Symantec Mail Security for SMTP to block email by a custom blacklist (which contains the sender's address or domain). It searches both the envelope From and message From headers to determine string matches.

An exact address match triggers a block first. If the exact address is not found, Symantec Mail Security for SMTP looks for the wildcard representation of the domain. If the wildcard representation of the domain is not found, it looks for the specific domain. If the specific domain is not found, Symantec Mail Security for SMTP strips the first portion of the domain, and the remaining portion is checked. This process continues until a match is found or until the entire domain is parsed.

Domain names must begin with either @ or a period. You can use wildcard characters in the user name portion of the address.

Note: If you configure Symantec Mail Security for SMTP to block a subdomain (server.company.com, for example), it blocks only that subdomain and not the full domain (company.com, for example).

To block by a custom blacklist

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.
2. In the Custom Blacklist window, under Blocking by sender's address, check **Identify messages from the following email addresses or domains as violations (one per line)**.
3. In the text box, type the email addresses and domains to be blocked.
   Use only one entry per line. Wildcard characters (* and ?) are allowed in the user name portion of an address.
4. Under Do the following when a violation occurs, select one of the following:
   - Drop message
   - Log only
   - Forward message
5. If you selected Forward message, in the To email address box, type the email address to which the message will be forwarded and in the Subject line box, type the subject that will appear in the subject line of the forwarded message.
6. Click **Save Changes**.

Identifying spam messages using the heuristic antispam engine

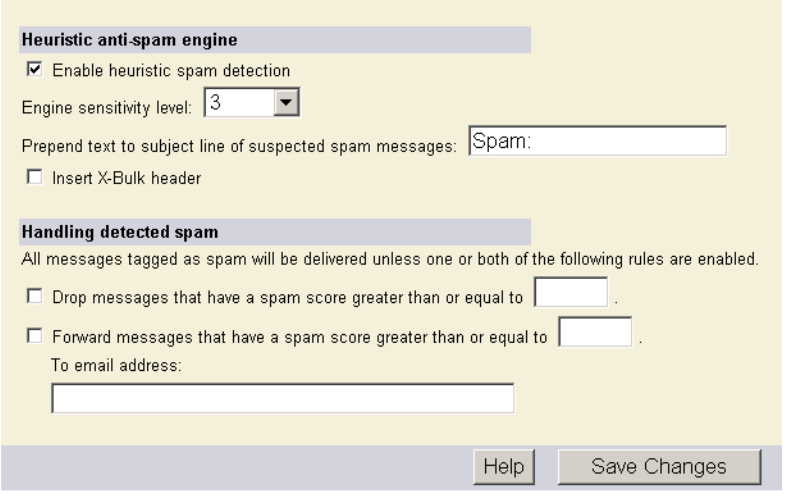
You can activate the heuristic antispam engine to detect spam. The heuristic antispam engine performs an analysis of the entire incoming email message, looking for key characteristics of spam. It weighs its findings against key characteristics of legitimate email and assigns a spam score (1-100) to show how certain it is that the message is spam. The higher the spam score, the more probable it is that the message is spam. This score, in conjunction with the engine sensitivity level (1=low, 5=high), determines whether a message is considered spam.

Note: The default sensitivity level for the heuristic antispam engine is 1. Increasing the sensitivity level may result in more false positives.

You can configure the handling of spam based on this score. You initially set the engine sensitivity level and spam score values. You may need to adjust these settings after you analyze your results over a period of time.

To identify suspected spam messages using the heuristic antispam engine

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.



2. In the Anti-Spam window, under Activating the heuristic antispam engine, check **Enable heuristic anti-spam detection**, and then select the engine sensitivity level.
3. Accept the default or type the text that you want to prepend the subject line of suspected spam messages.
4. Check **Insert X-bulk header** to add a default header name (X-Bulk: <space> spam score) to the MIME headers of all messages that have been detected as spam.
5. Under Handling detected spam, select any of the following rules and supply scores in one or both of the following boxes:
   - Drop messages that have a spam score greater than or equal to ___.
   - Forward messages that have a spam score greater than or equal to ___.

   The spam score for Forward must be less than the score for Drop if both are enabled.
6. Type an email address if the forward option is enabled.
7. Click **Save Changes**.

Identifying spam using Symantec Premium AntiSpam

In addition to providing real-time blacklisting and sender and recipient whitelisting, Symantec Premium AntiSpam uses the following to identify and handle spam:

Reputation service	Symantec monitors email sources to determine how much of the mail that is sent from those sources is legitimate. Email from those sources can then be blocked or allowed based on the reputation value of the source as determined by Symantec. Symantec uses the following lists to filter your messages: ■ Open proxy list: A dynamic database that contains the IP addresses of identity-making relays, including proxy servers with open or insecure ports. ■ Safe list: A list of IP addresses from which virtually no outgoing email is spam. ■ Suspect list: A list of IP addresses from which virtually all of the outgoing email is spam.
Suspected spam threshold	The premium antispam service calculates a spam score from 1 to 100 for each message. If a message scores from 90 to 100, it is defined as spam. This range is not configurable. For more aggressive filtering, you can define a spam threshold below 90 and above 24 to identify suspected spam. You specify actions for handling spam and suspected spam separately.
Language identification	The premium antispam service can determine the language in which a filtered message is written. You can configure the premium antispam service to automatically route messages that are written in certain languages to a spam folder in the recipient's mailbox. To use this feature, you must deploy the optional plug-in for Microsoft Outlook to the desktop computers on your network. The plug-in is available on the Symantec Mail Security for SMTP installation CD.

Filters	The premium antispam service supports the following types of filters: ■ URL filtering: Symantec builds its known-spammer list based on URLs that appear in spam. This list contains over 20,000 URLs. ■ Heuristic filtering: Heuristic filters scan the headers and the body of a message to test for characteristics that are usually inherent in spam, such as opt-out links, specific phrases, and forged headers. ■ Signature filtering: Messages that flow into the Symantec Brightmail Logistics and Operations Center (BLOC) are characterized using a unique signature that is added to the database of known spam. Using this signature, Symantec can group and match seemingly random messages that originated from a single attack.

See "Configuring Symantec Premium AntiSpam" on page 100.

See "Enabling language identification" on page 104.

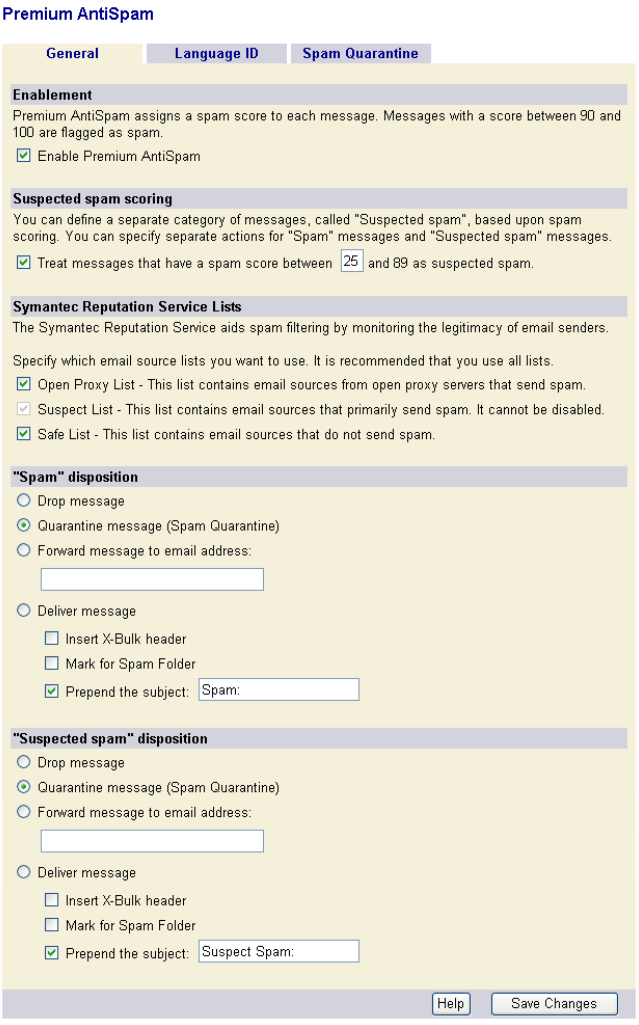
Configuring Symantec Premium AntiSpam

After you activate your Symantec Premium AntiSpam license, you must enable and configure the service to identify and handle spam and suspected spam.

See "Activating product and content licenses" on page 38.

To configure Symantec Premium AntiSpam

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.



2 In the Premium AntiSpam window, on the General tab, under Enablement, check **Enable Premium AntiSpam**.

To identify suspected spam

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.
2. In the Premium AntiSpam window, on the General tab, under Suspected spam scoring, check **Treat messages that have a spam score between [ ] and 89 as suspected spam**.
3. Accept the default of 72, or type a number between 25 and 89.
   Lowering the default may result in false positives.
4. Click **Save Changes**.

To configure the reputation service

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.
2. In the Premium AntiSpam window, on the General tab, under Symantec Reputation Service Lists, uncheck the check boxes for the lists that you do not want to use.
   Suspect List is checked by default and cannot be disabled.

To configure spam handling

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.
2. In the Premium AntiSpam window, on the General tab, under “Spam” disposition, select one of the following:
   - Drop message
   - Quarantine message (Spam Quarantine)
   - Forward message to email address
   - Deliver message

   A dropped message is accepted by the SMTP server, but it is then deleted. It is not delivered to the addressee.

3 Under Deliver message, select any of the following:

Insert X-Bulk header	X-Bulk:100 will be added to the MIME headers of all messages that have been detected as spam.
Mark for Spam Folder	You must have the Spam Folder Agent installed on the Exchange or Domino server through which you are routing the mail. An X-header will be added to let the agent move the message to the user's spam folder. It will display as X-bmifolder:1. You cannot modify this X-header.
Prepend the subject	You can accept the default (Spam) or replace it with other text.

4 Click Save Changes.

To configure suspected spam handling

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click Anti-spam Policy.

2 In the Premium AntiSpam window, on the General tab, under "Suspected Spam" disposition, select one of the following:

- Drop message
- Quarantine message (Spam Quarantine)
- Forward message to email address
- Deliver message

A dropped message is accepted by the SMTP server, but it is then deleted. It is not delivered to the addressee.

3 Under Deliver message, select any of the following:

Insert X-Bulk header	X-Bulk:89 will be added to the MIME headers of all messages that have been detected as suspected spam.
Mark for Spam Folder	You must have the Agent installed on the Exchange or Domino server through which you are routing mail for this to function. An X-header will be added to allow the Agent to move the message to the user's spam folder. It will display as X-bmifolder:1. You cannot modify this X-header.
Prepend the subject	You can accept the default (Spam) or replace it with other text.

4 Click **Save Changes**.

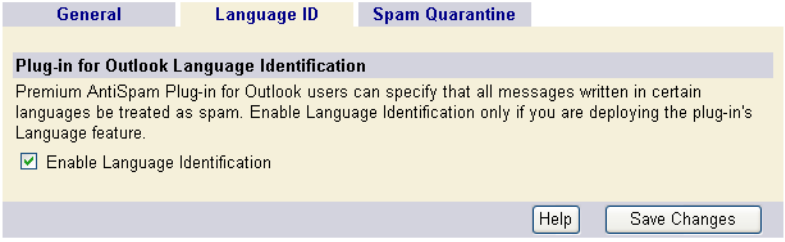
Enabling language identification

You can configure the premium antispam service to automatically route messages that are written in certain languages to a spam folder in the recipient's mailbox. When the premium antispam service detects that a message is written in one of these languages, it adds an X-header to the message. The X-header contains the information needed to deliver the message to the spam folder instead of to the inbox.

To use this feature, you must deploy the optional plug-in for Microsoft Outlook to the desktop computers on your network. The plug-in is available on the Symantec Mail Security for SMTP installation CD.

To enable language identification

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.



2 In the Premium AntiSpam window, on the Spam Quarantine tab, check **Enable Language Identification**.

3 Click **Save Changes**.

Configuring the spam quarantine

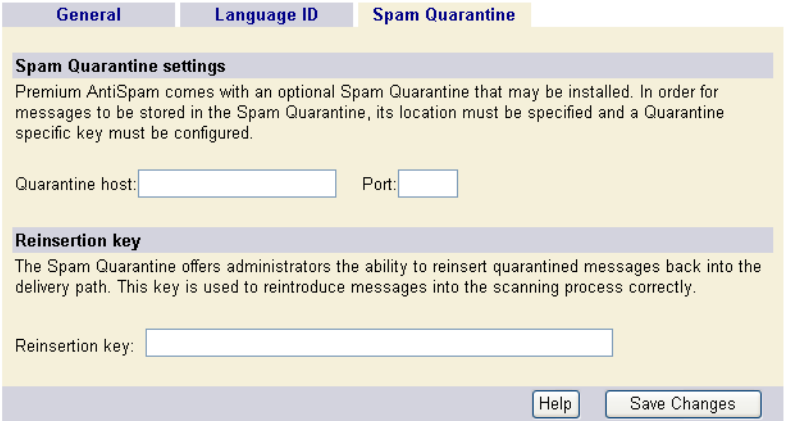
The spam quarantine lets users with Internet access browse, search, and delete their spam messages and deliver misidentified messages to their inboxes. An administrator account is required to access to all quarantine messages.

See "Creating administrator information" on page 106.

See "Accessing the spam quarantine" on page 119.

To configure the spam quarantine

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.



2 In the Premium AntiSpam window, on the Spam Quarantine tab, under Spam Quarantine settings, in the Quarantine host, type the IP address of the spam quarantine server.

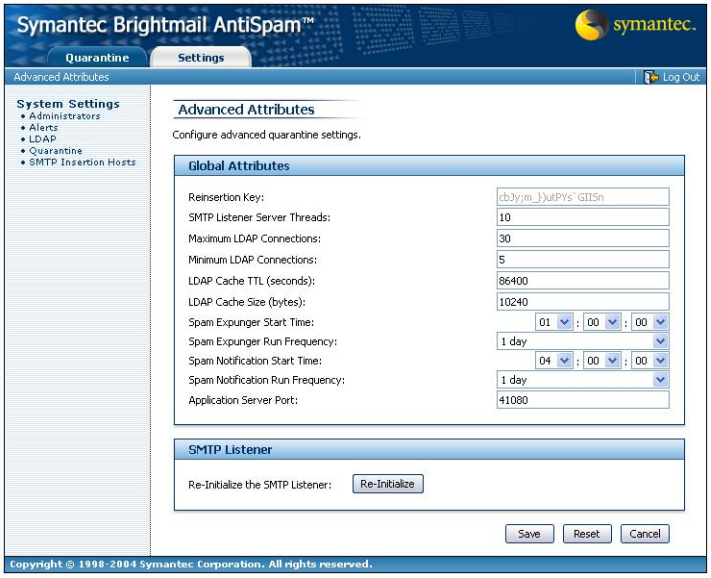
The quarantine host should be the server on which Symantec Mail Security for SMTP is installed.

3 In the Port box, type the port number of the spam quarantine server.

4 Under Reinsertion key, in the Reinsertion key box, paste the reinsertion key.

The reinsertion key is unique for each quarantine server. Do the following to retrieve the reinsertion key:

- Go to http://<QuarantineServer>:41080/brightmail/settings/advanced/editAdvancedSettings.do
- Under Global Attributes, copy the reinsertion key.



5 Click **Save Changes**.

Creating administrator information

You can create one or more administrator accounts through the Brightmail spam quarantine user interface.

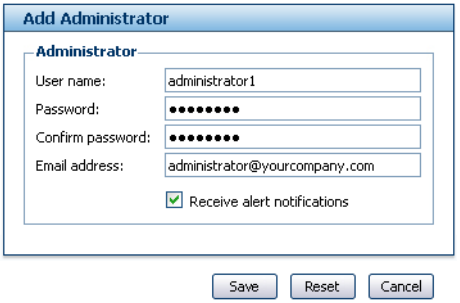
To access the Brightmail spam quarantine user interface

- On the Internet, go to http://<QuarantineServer>:41080/brightmail/viewLogin.do
  The user name is admin. The password is brightmail.

To add an administrator

1 On the Settings tab, in the left pane, under System Settings, click **Administrators**.

2 Click **Add**.



3 In the Add Administrator window, in the User name box, type a name for the administrator.

4 In the Password box, type a password.

5 In the Confirm password box, type the password again.

6 In the Email address box, type the email address for the administrator.

7 Click **Save**.

To edit an administrator's information

1 On the Settings tab, in the left pane, under System Settings, click **Administrators**.

2 In the Administrators window, select the administrator name that you want to edit.

3 Click **Edit**.

4 In the Edit Administrator window, edit the information.

5 Click **Save**.

To delete an administrator

1 On the Settings tab, in the left pane, under System Settings, click **Administrators**.

2 In the Administrators window, select the administrator name that you want to delete.

3 Click **Delete**.

Configuring alerts

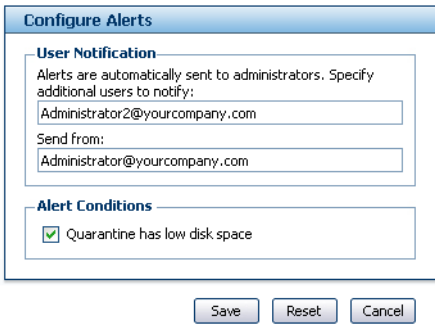
An alert is sent to administrators when the spam quarantine has low disk space. You can also specify users to receive the alert. This information is configured through the Brightmail spam quarantine user interface.

To access the Brightmail spam quarantine user interface

- On the Internet, go to http://<QuarantineServer>:41080/brightmail/viewLogin.do
  The user name is admin. The password is brightmail.

To configure alerts

1. On the Settings tab, in the left pane, under System Settings, click **Alerts**.



2. On the Alerts Settings window, under Configture Alerts, under User Notification, type the email addresses of users to whom alerts will be sent. Separate multiple addresses with commas (with no spaces between).
3. In the Send from box, type the email address from which the alert should appear to be sent.
4. Under Alert Conditions, check **Quarantine has low disk space**.
5. Click **Save**.

Configuring LDAP settings

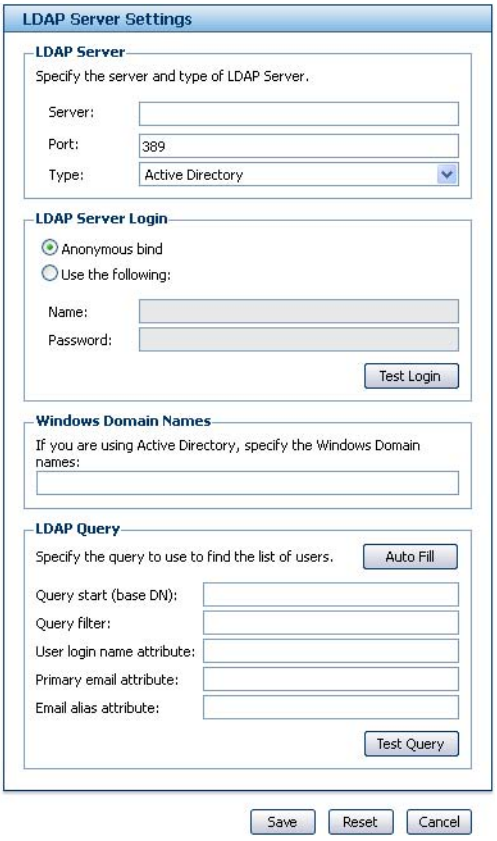
If you want users on your network to view their messages in the quarantine, you must configure the quarantine to access an LDAP directory, such as Active Directory or SunONE. If you don't have an LDAP directory or don't want users to access the quarantine, you can configure the quarantine for administrator-only access.

See "To configure quarantine settings" on page 113.

To configure LDAP settings for Active Directory

1 On the Internet, go to http://<QuarantineServer>:41080/brightmail/viewLogin.do
User name is admin. Password is brightmail.

2 On the Settings tab, in the left pane, under System Settings, click **LDAP**.



3 In the LDAP window, under LDAP Server, in the Server box, type the fully qualified domain name or IP address of an Active Directory domain controller, such as dc.example.com.
If you have a multi-domain Active Directory forest, specify the fully qualified domain name or IP address of the Global Catalog server on the root domain.

4 In the Port box, type the TCP/IP port for the Active Directory server.
Usually, the port is 389, which is the default port for LDAP servers.

5 In the Type box, click **Active Directory**.

6 Under LDAP Server Login, select **Anonymous bind** or **Use the following** to specify a user name and password.
Unless you have configured Active Directory to allow anonymous access, the Anonymous bind setting does not usually have adequate authentication privileges for the spam quarantine to access the necessary Active Directory information.

7 In the Name box, type the user name for an account that can authenticate as an administrator.
Type the user name using the format <NetBIOS>/<username>, for example, MSALPHA\Administrator

8 In the Password box, type the password for the account.
Logon credentials are required. If you do not want to type a user name and password, you must select Anonymous Bind.

9 Click **Test Login** to verify that the spam quarantine can authenticate against Active Directory using the information that you have supplied.
If you receive a status message that indicates that the test login to the LDAP server failed, you should review the information that you have specified and try again. Do not proceed until clicking Test Login yields a success message.

10 Under Windows Domain Names, type the NetBIOS domain names used by Active Directory.
If you have multiple domains, separate each entry with a semicolon, for example, MSAPLPHSA;MSBETA
If you specify multiple domains, users must select the appropriate NetBIOS domain from a list on the logon page when they log on to the spam quarantine.

11 Under LDAP Query, click **Auto Fill** to fill in the boxes in the LDAP Query section using the information that you have already supplied.

12 Click **Test Query** to determine if the quarantine can access the required user information using the settings that you supplied.
If the test is unsuccessful, an error message that describes the problem is displayed.

13 If the test query was successful but the response time is slow, or if your site has multiple domains, in the Query start (base DN) box, edit the Base DN entry so that it is more specific, for example, by specifying the CN or OU.
For example:
CN=users,DC=msalpha,DC=com or OU=marketing,DC=msalpha,DC=com
If you have multiple OUs or domains, use an ampersand (&) to separate each entry, for example, DC=msalpha,DC=com&DC=msbeta,DC=com

14 If the test query was unsuccessful, verify the following information:

Query filter	Ensure that the query filter includes the values from User login name attribute, Primary email attribute, and Email alias attribute as wildcard searches. These values are filled in when you select Auto Fill. The default value for Active Directory is (&(| (objectCategory=group) (objectCategory=person)) (&(| (mail=*) (proxyAddresses=*)) (sAMAccountName=*)))
User login name attribute	You may need to modify this entry. The default for Active Directory is sAMAccountName
Primary email alias attribute	You may need to modify this entry. The default for Active Directory is mail
Email alias attribute	You may need to modify this entry. The default for Active Directory is proxyAddresses

15 Click **Save**.

16 Attempt to log on to the spam quarantine.

To configure LDAP settings for iPlanet, SunONE, or Java Directory Server

1 On the Settings tab, in the left pane, under System Settings, click **LDAP**.

2 In the LDAP window, under LDAP Server, in the Server box, type the fully qualified domain name or IP address of the LDAP server, for example, ldap.example.com

3 In the Port box, type the TCP/IP port for the Active Directory server. Usually, the port is 389, which is the default port for LDAP servers.

4 In the Type box, click **iPlanet/Sun ONE/Java Directory Server**.

5 Under LDAP Server Login, select **Anonymous bind** or **Use the following** to specify a user name and password.
Unless you have configured LDAP to allow anonymous access, the Anonymous bind setting does not usually have adequate authentication privileges for the spam quarantine to access the necessary LDAP information.

6 In the Name box, type the user name for an account that can authenticate as an administrator.
For iPlanet, SunONE, or Java Directory Server, the default administrator is cn=Directory Manager.

7 In the Password box, type the password for the account.
Logon credentials are required. If you do not want to type a user name and password, you must select Anonymous Bind.

8 Click **Test Login** to verify that the spam quarantine can authenticate against LDAP using the information that you have supplied.
If you receive a status message that indicates that the test login to the LDAP server failed, you should review the information that you have specified and try again. Do not proceed until clicking Test Login yields a success message.

9 Leave the Windows Domain Names box blank.

10 Under LDAP Query, click **Auto Fill** to fill in the boxes in the LDAP Query section using the information that you have already supplied.

11 Click **Test Query** to determine if the quarantine can access the required user information using the settings that you have supplied.
If the test is unsuccessful, an error message that describes the problem is displayed.

12 If the test query was successful but the response time is slow, or if your site has multiple domains, in the Query start (base DN) box, edit the Base DN entry so that it is more specific, for example, by specifying the CN or OU.
For example:
CN=users,DC=msalpha,DC=com or OU=marketing,DC=msalpha,DC=com
If you have multiple OUs or domains, use an ampersand (&) to separate each entry, for example, DC=msalpha,DC=com&DC=msbeta,DC=com

13 If the test query was unsuccessful, verify the following information:

Query filter	Ensure that the query filter includes the values from User login name attribute, Primary email attribute, and Email alias attribute as wildcard searches. These values are filled in when you select Auto Fill. The default value for SunONE Directory Server is (&(| (objectClass=inetMailGroup) (objecgtClass=person)) (| (mail=*) (mailalternateaddress=*)))
User login name attribute	You may need to modify this entry. The default value for SunONE is mail
Primary email attribute	You may need to modify this entry. The default value for SunONE is mail
Email alias attribute	You may need to modify this entry. The default value for SunONE is mailAlternateAddress

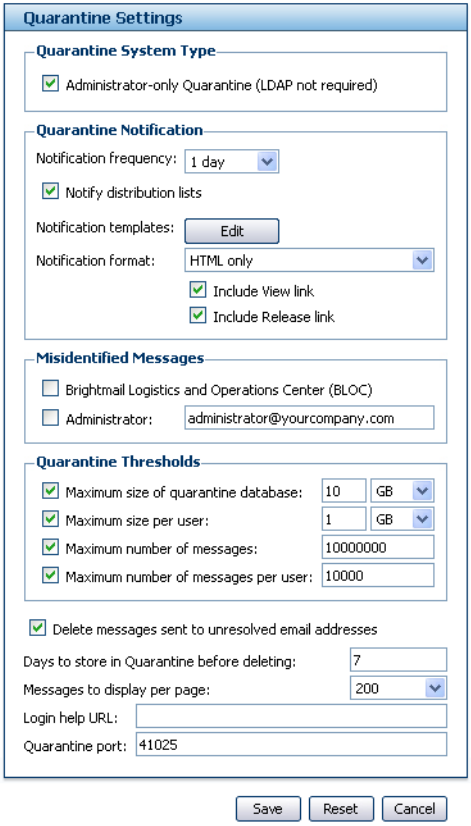
14 Click **Save**.

15 Attempt to log on to the spam quarantine.

To configure quarantine settings

1 On the Internet, go to http://<QuarantineServer>:41080/brightmail/viewLogin.do
User name is admin. Password is brightmail.

2 On the Settings tab, in the left pane, under System Settings, click **Quarantine**.



3 In the Quarantine Settings window, under Quarantine System Type, check **Administrator-only Quarantine**.
When administrator-only access is enabled, you can still perform all administrator tasks, which includes redelivering misidentified messages to local users. However, notification of new spam messages is disabled when administrator-only access is enabled.

4 In the Quarantine Notification drop-down list, select how frequently you would like to receive quarantine notifications.
By default, a notification process runs at 4 A.M. every day to determine if users have new spam messages in the quarantine. If so, it sends a message to users who have new spam to remind them to check their spam messages in the quarantine.
You can edit the notification template.
See "Editing the notification templates" on page 114.

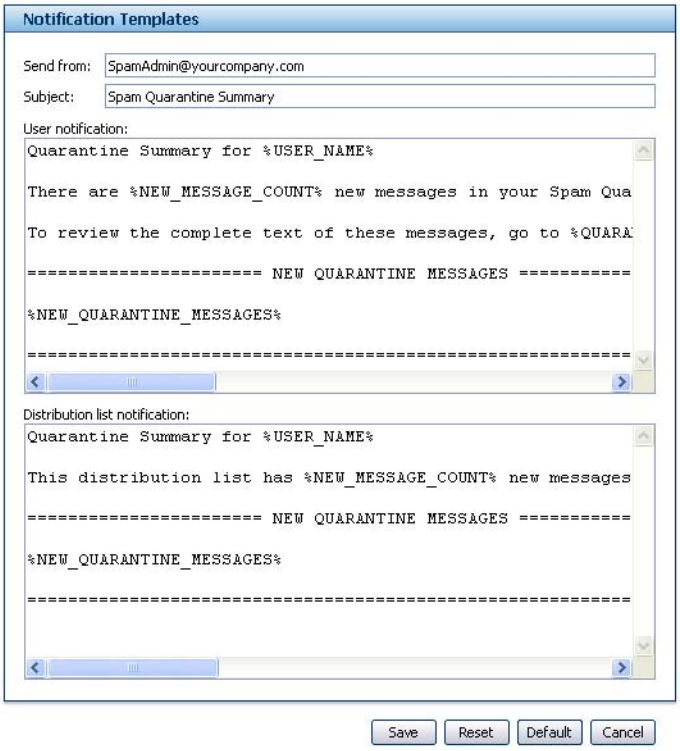
5 Check **Notify distribution lists** if you would like for users on distribution lists to receive notification digests.

Editing the notification templates

You can edit the notification templates that are used for email notifications that users and distribution lists receive when their incoming messages are quarantined.

To edit the notification templates

1 Beside Notification templates, click **Edit** to edit the template.



- In the Send from box, type the email address from which the notification digests should appear to be sent.
  You should type an address to which users can send questions about the notification digests. Specify the full email address including the domain name, for example, admin@corp.com
- In the Subject box, type the text that should appear in the Subject header of notification digests, for example, Your Suspected Spam Summary.
  Do not put message variables in the subject box. They will not be expanded.

2 Edit the user notification template, the distribution lists notification template, or both using the following variables:

%NEW_MESSAGE_COUNT%	Number of new messages in the user's spam quarantine since the last notification message was sent.
%NEW_QUARANTINE_MESSAGES%	List of messages in the user's quarantine since the last notification was sent. For each message, the contents of the From, Subject, and Date headers are printed. View and Release links are displayed for each message if they are enabled and you have chosen Multipart or HTML notification format.
%QUARANTINE_DAYS%	Number of days that messages in the Quarantine will be kept. After that period, messages will be purged.
%QUARANTINE_URL%	URL that the user clicks to display the quarantine logon page.
%USER_NAME%	User name of the user receiving the notification message.

3 In the Notification format drop-down list, select one of the following:

Multipart (HTML and text)	Send a notification message in MIME multipart format. Users will see either the HTML version or the text version, depending on the type of email client that they are using and the email client settings. The View and Release links do not appear next to each message in the text version of the summary message.
HTML only	Send the notification message in MIME type text/html only.
Text only	Send the notification message in MIME type text/plain only. If you select Text only, the View and Release Links do not appear next to each message in the summary message.

4 Check **Include View link** to include a View link next to each message in the notification digest message summary.
If you remove the %NEW_QUARANTINE_MESSAGES% variable from the notification digest template, the new message summary, including the View links, will not be available.

5 Check **Include Release link** to include a Release link next to each message in the notification digest message summary.
The Release link is for misidentified messages. When a user releases a notification digest message, the adjacent message is released from the quarantine and sent to the user's normal inbox.
If you remove the %NEW_QUARANTINE_MESSAGES% variable from the notification digest template, the new message summary, including the Release links, will not be available.

6 Under Misidentified Messages, check **Brightmail Logistics and Operations Center (BLOC)** to report misidentified messages to Symantec.
The BLOC analyzes message submissions to determine if the filters need to be changed. The BLOC will not send confirmation of the misidentified message submission to the administrator or the user who submits the message.

7 Check **Administrator** and type a full email address (including domain name) of someone who will monitor misidentified messages at your organization.
A copy of the misidentified messages will be sent to this address.

8 Under Quarantine Thresholds, select any of the following:

Maximum size of quarantine database	Maximum amount of disk space used for quarantined messages for all users. When a new message arrives after the threshold has been reached, the 10 oldest messages are deleted, and the new message is kept.
Maximum size per user	Maximum amount of disk space used for quarantine messages per user. When a new message arrives after the threshold has been reached, the 10 oldest messages of the user are deleted, and the new message is kept.
Maximum number of messages	Maximum number of messages for all users. (The same message sent to multiple recipients counts as one message.) When a new message arrives after the threshold has been reached, the oldest message is deleted, and the new message is kept.
Maximum number of messages per user	Maximum number of quarantine messages per user. When a new message arrives after the threshold has been reached, the user's oldest message is deleted, and the new message is kept.

9 Check **Delete messages sent to unresolved email addresses** to delete quarantined messages that are sent to non-existent email addresses.

10 In the Days to store in Quarantine before deleting box, type the number of days that spam messages are kept before being deleted.
By default, a quarantine process runs at 1 A.M. every day to delete messages that are older than the retention period. Each time the process runs, 10,000 messages, at most, can be deleted.

11 In the Messages to display per page drop-down list, select how many lines of messages to display on the message list page for administrators and users.

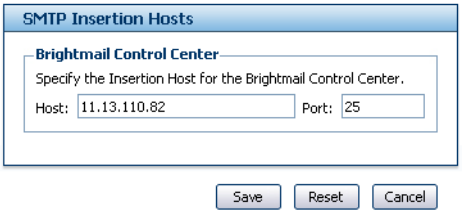
12 Optionally, in the Login help URL box, type the URL to your custom Web page.
You can create a Web page that tells your users how to log on and make it available on your network. The Web page should be accessible from any computer where users will log on to the spam quarantine.
If you leave this box empty, when a user clicks **Need help logging in**, online help from Symantec is displayed in a new window.

13 In the Quarantine port box, type the port number from which the quarantine will accept messages.
By default, the port is 41025.

14 Click **Save**.

To configure SMTP insertion hosts

1 On the Settings tab, in the left pane, under System Settings, click **SMTP Insertion Hosts**.



2 In the SMTP Insertion Hosts window, in the Host box, type the IP address of the computer on which Symantec Mail Security for SMTP is installed.
Symantec Mail Security for SMTP will deliver all messages that are released to the inbox by the quarantine users, send email notification when alerts are generated, and send spam notifications to users.

3 In the Port box, type the port number of the computer on which Symantec Mail Security for SMTP listens.

4 Click **Save**.

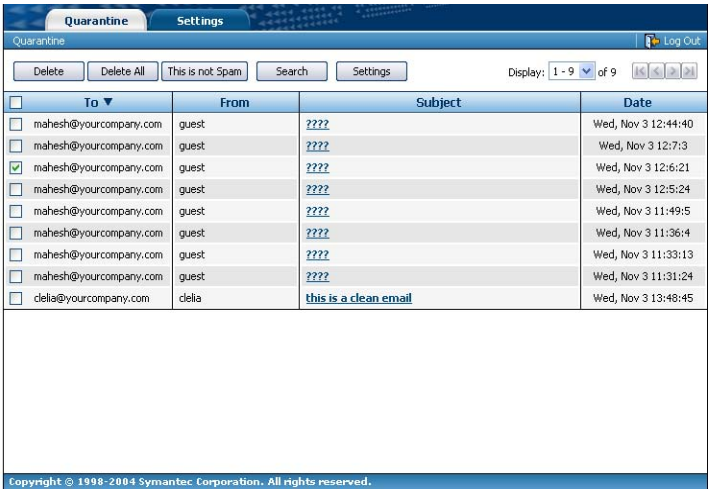
Accessing the spam quarantine

Administrators can access the spam quarantine to do the following:

- Sort messages
- View messages
- Redeliver misidentified messages
- Delete messages
- Search messages

To sort messages

1 On the Internet, go to http://<QuarantineServer>:41080/brightmail/quarantine/viewInbox.do



2 Click the column heading on which you want to sort.
A triangle appears in the selected column that indicates ascending or descending sort order.

3 Click the selected column heading again to switch between ascending and descending order.

To view messages

- In the Subject column, click the message subject that you want to view.

To redeliver misidentified messages

1. In the To column, check the check box to the left of a misidentified message.
2. Click **This is not Spam**.
   If the reinsertion key has been entered in Symantec Mail Security for SMTP, when an administrator clicks **This is not Spam**, the message is removed from the spam quarantine and delivered to the intended recipient. When a user clicks **This is not Spam**, the message is delivered to the user's inbox. Each reinsertion key is unique to a spam quarantine server. When an administrator clicks **This is not spam**, the message is sent to the reinsertion host. Symantec Mail Security for SMTP attempts to match the reinsertion key that the spam quarantine server assigned to the one that is entered in Symantec Mail Security for SMTP. If the keys match, the message bypasses the antispam engines and is delivered to the recipient's inbox. If the keys do not match, the message is rescanned and redetected as spam. It is then handled according to the disposition settings.

To delete individual messages

1. In the To column, check the check box to the left of each message to be deleted.
2. Click **Delete**.
   Deleting a message in the administrator's spam quarantine also deletes the message from the user's spam quarantine. Users can view and delete only their own spam messages.

To delete all messages

1. Click **Delete All**.
2. In the confirmation window, click **OK**.

To search messages

1. Click **Search**.
2. Under Search Criteria, type text in one or more boxes, and, optionally, from the time range menu, choose a time range.
3. Click **Search**.

Blocking by custom spam rules

You can create spam rules to be used for processing. The operators that are allowed to separate terms are AND, OR, and NOT. (NOT implies AND NOT.) The terms AND and OR cannot be mixed within a single filtering statement. Multiple NOT operators are allowed within a single filtering statement. AND can also be delimited by a comma. By selecting All of these terms or Any of these terms from the menu, the operators are determined. (All of these terms=AND. Any of these terms=OR.)

To block by custom spam rules

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Anti-spam Policy**.
2. In the Spam Rules window, on the Status tab, select **Enable message body scanning for both Spam and Content Violation Rules**.
3. Click **Save Changes**.
4. On the Spam tab, under Spam filtering rules, click **Add**.
5. Under Custom filtering rule definition, select **Enable this custom filtering rule**.
6. In the drop-down list, select one of the following:
   - All of these terms
   - Any of these terms
7. In the Identify messages that contain box, type one or more terms to be used for filtering.
   Separate all terms with commas. If you are typing phrases, type all words in the phrase without commas between them.
   Terms are not case-sensitive by default.
   All characters (including whitespaces) are matched literally except for the following:

*	Matches 0 or more characters
?	Matches exactly one character
\	Escapes any special meaning for * and ?

   The maximum number of terms within a single rule is 50. The maximum number of spam and content rules combined is 100.

8 If desired, in the None of these terms box, type the terms to be used to identify that a message is not spam.

If a term is in the Not field and a message is sent that has all of the blocked terms (AND/OR portion of rule) but also has a Not term, the message will not be in violation of the rule. (It will not be considered spam.)

9 Click **Save**.

Chapter 6

Setting your filtering policy

This chapter includes the following topics:

About your filtering policy

Your filtering policy is determined by how you configure Symantec Mail Security for SMTP to filter messages (which criteria to use to block messages and attachments and how those blocked messages and attachments should be handled).

Table 6-1 shows the criteria that you can use to filter messages and attachments and how those filtered messages and attachments can be handled.

Table 6-1 Filtering criteria

Criteria	Handling options
Message size	Email messages that exceed the size that is specified in megabytes are not accepted at the SMTP server. Not blocking messages based on size is the default.
Subject line	Email messages with specified subject lines may be dropped, logged, or forwarded. Not identifying subject lines is the default.
File name	Email messages with specified file names may be delivered with their attachments deleted. Not deleting attachments based on file names is the default, although a suggested extension list is provided.
Container limit	Email messages that exceed any of the specified container limits may be dropped. Blocking messages that exceed container limits is the default.
Encrypted container	Email messages that are encrypted or password-protected have their containers deleted and the messages delivered; the messages and containers dropped; the incidents logged and the messages with containers delivered; or the messages and containers forwarded to a specified address. Deleting the containers and delivering the messages is the default.
Anti-relay settings	Email messages with non-local destinations are handled according to how you configure Symantec Mail Security for SMTP. Do not allow, except for listed hosts is the default.
Content rules	Email messages in which content violation filtering rules are detected are handled according to how the product is configured.

Blocking by content

Symantec Mail Security for SMTP can be configured to block messages based on the following content:

- Message size
  See "Blocking by message size" on page 127.
- Subject line
  See "Blocking by subject line" on page 127.
- File name
  See "Blocking by file name" on page 128.

Blocking by message size

You can configure Symantec Mail Security for SMTP to block email by message size.

To block by message size

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Filtering Policy**.
2. In the Content window, under Blocking by message size, check **Reject messages that are greater than [ ] megabytes**.
   The default is 50.
3. In the text box, type the number of megabytes that must be exceeded for a message to be rejected.
   Do not use a decimal.
4. Click **Save Changes**.

Blocking by subject line

You can configure Symantec Mail Security for SMTP to block email by subject line.

To block by subject line

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Filtering Policy**.
2. In the Content window, under Blocking by subject line, check **Identify the following subject lines (one per line) as content violations**.

3 In the subject line box, type the subject lines (one per line) that Symantec Mail Security for SMTP should block.

You can use the * and ? wildcard characters. The * wildcard character matches 0 or more of any character. The ? wildcard character blocks any 1 (exactly 1) character.

For example, *hot* would block any subject line that contains those three letters consecutively in the line (For example, any line that contains the word shotgun would be blocked.) The wildcard string ?hot? would block the subject line shots, but not hot, hots, or a line that contains any of those words.

(Using the ? wildcard character to match a high ASCII character does not result in a block.)

Subject-line blocking is not case-sensitive. Fw: and Re: are added automatically by the software.

4 Under Take the following action when a subject line violation occurs, select one of the following:

- Drop message
- Log only
- Forward message

5 If you selected Forward message, in the To email address box, type one address to which the blocked message will be forwarded, and then, in the Subject line box, type the subject line of the rejected message to be forwarded.

6 Click **Save Changes**.

Blocking by file name

You can configure Symantec Mail Security for SMTP to block email by file name. You can delete file names from the default list or add more file names to be blocked.

Table 6-2 shows the extensions (with * as a wildcard character) that Symantec Mail Security for SMTP blocks by default when you enable blocking by file name.

Table 6-2 Default extension blocking list

File extension	Description
*.ad	After Dark screen saver file
*.ade	Microsoft Access Project extension
*.adp	Microsoft Access Project

Table 6-2 Default extension blocking list

File extension	Description
*.asp	Active Server Pages file
*.bas	Visual Basic® Class module
*.bat	Batch file
*.chm	Compiled HTML Help file
*.cmd	Win32 command script
*.com	MS-DOS® application
*.cpl	Control Panel extension
*.crt	Security certificate
*.exe	Win32 application
*.hlp	Windows Help file
*.hta	HTML application
*.inf	Setup information file
*.ins	Internet communication settings
*.isp	Internet communication settings
*.js	JScript® file
*.jse	JScript encoded script file
*.lnk	Shortcut
*.mdb	Microsoft Access database
*.mde	Microsoft Access MDE database
*.msc	Microsoft common console document
*.msi	Windows installer package
*.msp	Windows installer patch
*.mst	Visual test source file
*.pcd	Photo CD image
*.pif	Shortcut to MS-DOS program
*.reg	Registration entries
*.scr	Screen saver

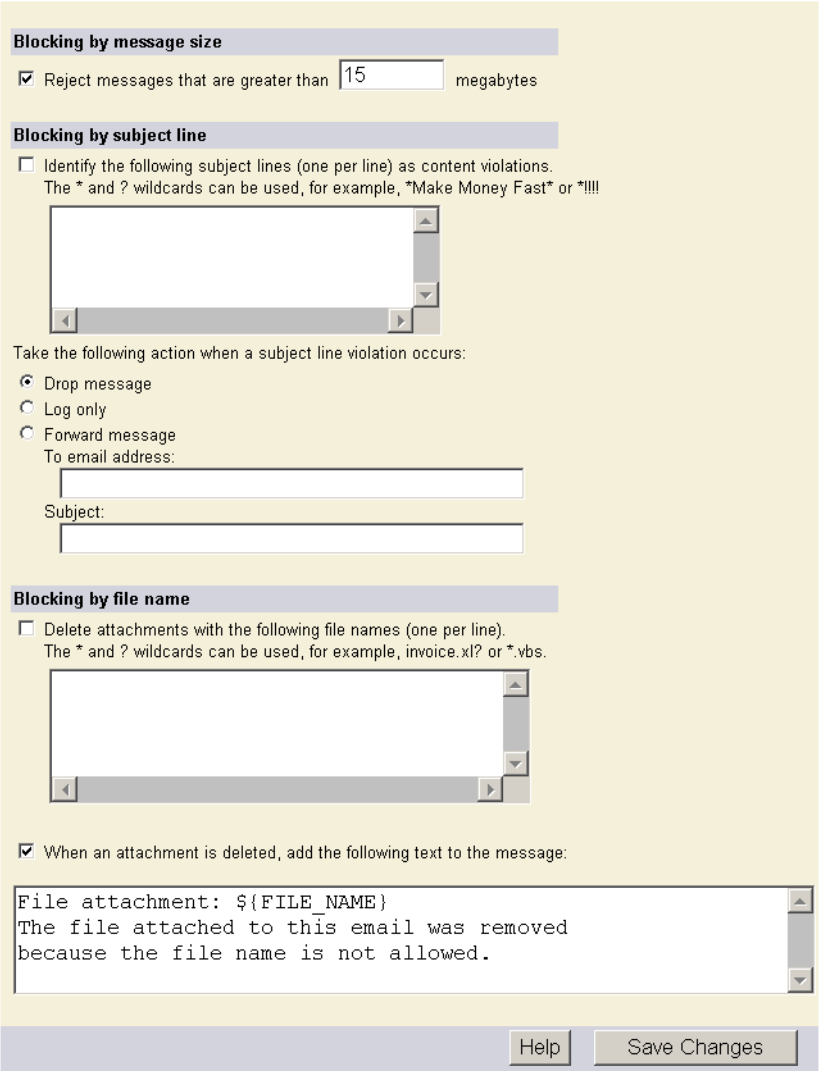
Table 6-2 Default extension blocking list

File extension	Description
*.sct	Windows script component
*.shb	Document shortcut file
*.shs	Shell scrap object
*.url	Internet shortcut (Uniform Resource Locator)
*.vb	VBScript file
*.vbe	VBScript encoded script file
*.vbs	VBScript script file
*.vsd	Visio® drawing file
*.vss	Visual SourceSafe file
*.vst	Targa bitmap file
*.vsw	Visio workspace file
*.ws	WordStar file
*.wsc	Windows script component
*.wsf	Windows script file
*.wsh	Windows scripting host settings file

Note: Typing only * or *.* will generate an error message.

To block by file name

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Filtering Policy**.



2 In the Content window, under Blocking by file name, check **Delete attachments with the following file names (one per line)**.
Even though the blocking list is populated with default file names to be blocked, Symantec Mail Security for SMTP will not block attachments with those file names unless you check **Delete attachments with the following file names**.

3 Type the file names that you want to block. Type one file name per line using the following format:
badnews.doc
You can use * for the file name or the extension.

4 To delete a default file name, select and delete the file name.

5 Check **If an attachment is deleted, add the following text to the message**.
You can customize the message, if needed.

6 Click **Save Changes**.

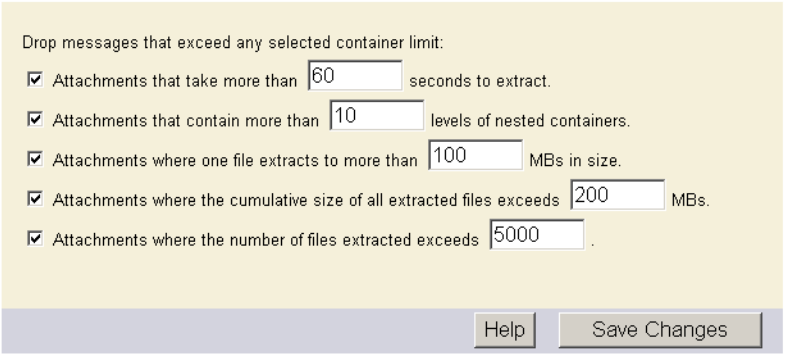
Blocking by container file limits

You can configure Symantec Mail Security for SMTP to protect against denial-of-service attacks that are associated with overly large container files that take a long time to decompose, or with files that contain multiple compressed files.

Note: Each message is treated as a container, meaning that the settings apply on a per message basis instead of on a per attachment basis. MIME headers are considered files.

To block by container file limits

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Filtering Policy**.



2 In the Container Limits window, select the container limit descriptors that you want to use for determining exceeded container limits.

3 Type the maximum allowable number for each enabled descriptor, or keep the defaults.

Do not type a zero (0) for the value.

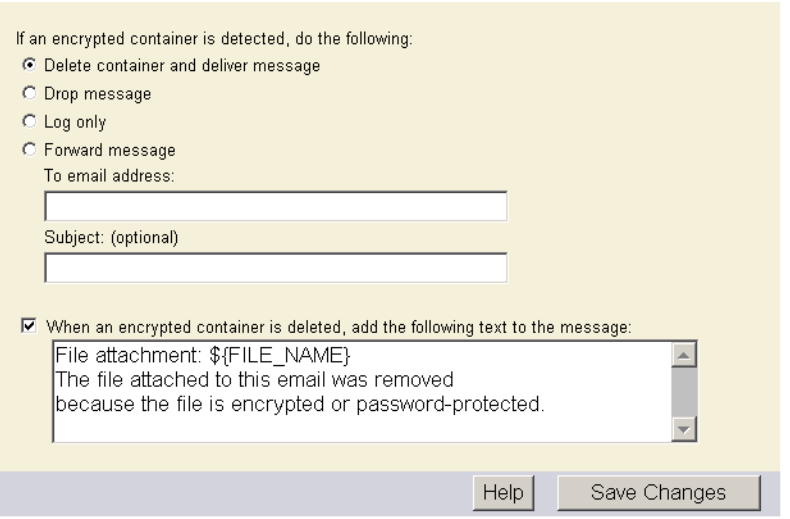
4 Click **Save Changes**.

Blocking if an encrypted container is detected

You can configure Symantec Mail Security for SMTP to handle encrypted container files.

To block if an encrypted container is detected

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Filtering Policy**.



2 In the Encrypted Container window, select one of the following:

- Delete container and deliver message
- Drop message
- Log only
- Forward message

3 If you selected Forward message, in the To email address box, type the email address to which the message with the encrypted container should be forwarded and in the Subject box, type the subject that will appear in the subject line of the forwarded message.

4 Click **Save Changes**.

Preventing relaying

You can configure relay restrictions within Symantec Mail Security for SMTP so that it refuses to deliver email that has a source outside of the organization (email for which the sender or recipient is not local).

Another way that Symantec Mail Security for SMTP prevents relaying is by rejecting messages to recipients with addresses that contain specific characters, such as ! and %.

Configuring external relay restrictions

The following relay options are available:

- Allow: Relay restrictions are turned off for external hosts. Email from any remote host can be relayed through Symantec Mail Security for SMTP to remote hosts.
- Do not allow, except for listed hosts (one per line): Relay restrictions are enabled for external hosts. Only email from explicitly named hosts and domains can be relayed to remote hosts.
  Do not allow, except for listed hosts (one per line) is the default.

The source of a message is the computer that contacts Symantec Mail Security for SMTP, not the From address. The destination is the host portion of the recipient's address. If the source or destination is considered local, the Do not allow setting does not apply.

See "To configure external relay restrictions" on page 136.

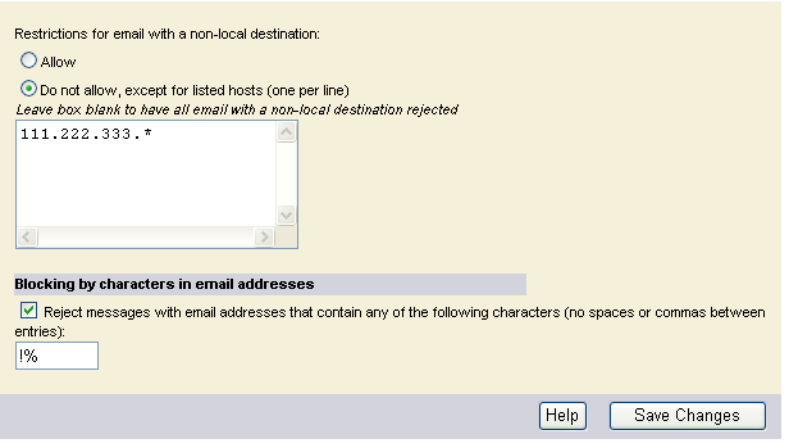
A source is considered local if Symantec Mail Security for SMTP is running in Allow mode or if the host is listed in the Do not allow list, except for listed hosts list.

A destination is considered local if it is listed in the Local Routing list.

See "Configuring local routing" on page 64.

To configure external relay restrictions

1 On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Filtering Policy**.



2 In the Anti-Relay window, select one of the following:

- Allow
- Do not allow, except for listed hosts (one per line)

3 If desired, type one host name, IP address, or domain per line for mail servers from which email will be allowed.
Domain name entries in this box will work only if the hosts have appropriate PTR records.
You can use the * wildcard character as the first element of a domain name or the last element of an IP address to specify allowed hosts. For example:
*.someplace.com
1.2.3.*
1.2.*
1.*
If Do not allow is selected, and no hosts are listed, Symantec Mail Security for SMTP rejects all email with a non-local destination.

4 Click **Save Changes**.

Blocking by characters in email addresses

You can configure Symantec Mail Security for SMTP to reject messages with email addresses that contain characters that are commonly associated with spam relaying, such as ! and %.

To block by characters in email addresses

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Filtering Policy**.
2. In the Anti-Relay window, under Blocking by characters in email addresses, check **Reject messages with email addresses that contain any of the following characters**.
3. In the text box, type one or more characters for which Symantec Mail Security for SMTP will search for email addresses to block.
   Do not insert spaces or commas between the entries.
4. Click **Save Changes**.

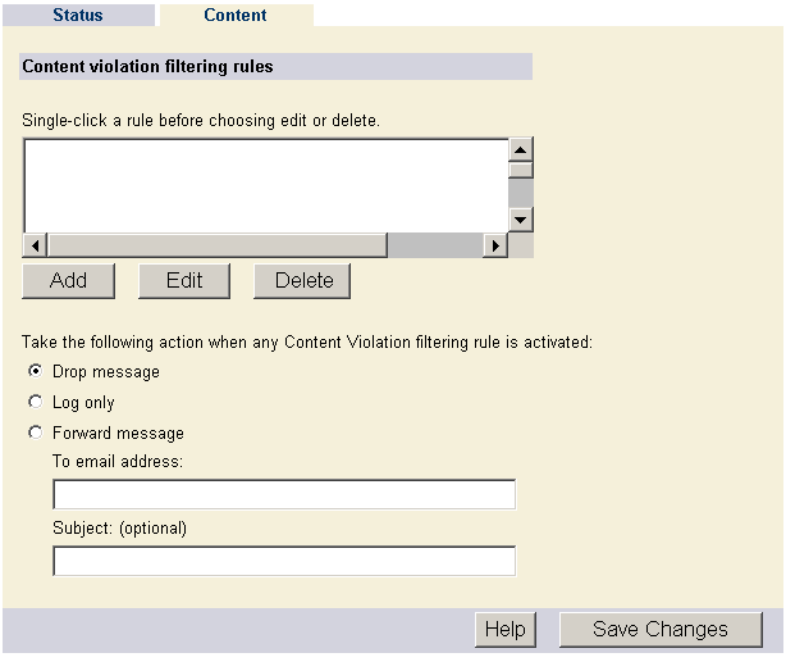
Blocking by custom content rules

You can create content rules to be used for processing. The operators that are allowed to separate terms are AND, OR, and NOT. (NOT implies AND NOT.) The terms AND and OR cannot be mixed within a single filtering statement. Multiple NOT operators are allowed within a single filtering statement. AND can also be delimited by a comma. By selecting All of these terms or Any of these terms from the menu, the operators are determined. (All of these terms=AND, Any of these terms=OR.)

To create a custom content rule

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Filtering Policy**.
2. In the Content Rules window, on the Status tab, check **Enable message body scanning for both Spam and Content Violation Rules**.

3 Click **Save Changes**.



4 On the Content tab, under Content filtering rules, click **Add**.

5 Under Custom filtering rule definition, check **Enable this custom filtering rule**.

6 In the drop-down list, select one of the following:

- All of these terms
- Any of these terms

7 In the Identify messages that contain box, type one or more terms to be used for filtering.

Separate all terms with commas. If you want to add phrases, type all words in the phrase without commas between them.

Terms are not case-sensitive by default.

All characters (including spaces) are matched literally except for the following:

*	Matches 0 or more characters
?	Matches exactly one character
\	Escapes any special meaning for * and ? only

The maximum number of terms within a single rule is 50. The maximum number of spam and content rules combined is 100.

8 Click **Save**.

9 On the Content tab, select the action to take when a content violation filtering rule is activated.

10 If you selected Foward message, type the email address to which the message should be sent.

The subject line is optional.

11 Click **Save Changes**.

Chapter 7

Logging and reporting

This chapter includes the following topics:

About the Status page

When you log on to Symantec Mail Security for SMTP, the Status page is displayed. This page shows system metrics that were calculated from the time of the most recent startup.

At the bottom of the window, you can click Refresh to update the display to reflect current, real-time status.

Note: Symantec Mail Security for SMTP attempts a separate delivery for each recipient and the results are tracked individually. On the Status page, the number of Messages Delivered is often greater than the number of Messages Accepted because of multiple recipients.

Table 7-1 shows the information that appears on the Status page.

Table 7-1 Status page information

Topic	Information
System status	■ Server and port number for Symantec Mail Security for SMTP. ■ Version number of the product <product license status:Valid or Invalid>. ■ Content license status: Valid or Invalid. ■ Premium AntiSpam license: Valid or Invalid. ■ Date on which the server was last started. ■ Amount of time that the server has been running since it was last started. ■ Status of virus scanning: Enabled or Disabled. ■ Status of Central Quarantine forwarding: All Files, Unrepairable Files, or Disabled. ■ Total number of megabytes that have been received for processing since the server was last started. ■ Message delivery mode: Delivery or Pause. ■ Incoming message status: Accept or Reject. ■ Date of last virus definitions update (and latest revision number). ■ Date of last premium antispam definitions update. This information displays only when the Symantec Premium AntiSpam license is valid. ■ Date of last spam definitions update (and latest revision number). This information displays only when the Symantec Premium AntiSpam license is invalid. ■ Date on which the SSL certificate was installed, or Not installed. ■ Total number of repaired, deleted, and logged viruses. ■ Total number of spam messages detected. ■ Total number of auto-generated whitelist entries. ■ Total number of policy violations.

Table 7-1 Status page information

Topic	Information
Messages	■ Accepted: Number of messages added to the fast queue since the server was last started. ■ Rejected: Number of messages rejected because the software is configured to reject messages; disallowed characters are in an email address; an anti-relay violation occurs; or the configured message size has been exceeded. ■ Delivered: Number of outgoing messages that have been delivered (including messages spawned internally by Symantec Mail Security for SMTP, such as bounce messages, delivery failure notifications, and configured notifications). ■ Forwarded: Number of messages that have been forwarded successfully to the administrator addresses See "To set administrator email addresses for notifications and alerts" on page 48. ■ Dropped: Number of messages dropped because the software is configured to drop messages in any of the following cases: attachments are not repaired or deleted; subject lines are disallowed; container limit has been exceeded; encrypted container has been detected; disallowed sender's address has been detected; block by antispam list, scan error, scan failure. ■ Held: Number of messages that have been added to the hold queue since the last restart, including those dropped by the administrator. ■ Quarantined: Number of files that have been added to the Central Quarantine. ■ Mass mailers deleted: Total number of messages dropped due to detection of mass-mailer worm infection.
Infections	■ Repaired: Number of files that had viruses repaired. ■ Deleted: Number of files that had viruses deleted. ■ Logged: Number of files that had viruses logged only.
Attachments	■ Number of top-level attachments that have been stripped from a message. ■ Number of encryptions deleted. ■ Number of encryptions logged.
Queue status	■ Number of messages currently in the fast queue. ■ Number of messages currently in the slow queue. ■ Number of messages currently in the hold queue.

Table 7-1 Status page information

Topic	Information
Antispam detections	■ Number of spam messages detected by the custom blacklist. ■ Number of spam messages detected by the real-time blacklist. ■ Number of spam messages detected by the heuristic antispam engine. This information displays only when the Symantec Premium AntiSpam license is invalid. When the premium antispam license is valid, the following will appear in place of the heuristic antispam engine entry: Spam, Suspected Spam, and Reputation Spam.

Generating reports

Symantec Mail Security for SMTP generates the following types of reports:

- Summary: Shows totals for message, infection, and virus activity. When viruses are found, it includes links to more information about the viruses. If the Symantec Premium AntiSpam license is valid, the summary report shows totals for spam, suspected spam, and reputation spam. If the Symantec Premium AntiSpam license is invalid, no spam information is reported.
  See "Generating summary reports" on page 145.
- Detail: Shows detailed information about message, infection, and virus activity (to include dates of occurrences and client IP addresses, for example).
  See "Generating detail reports" on page 148.

Generating summary reports

The summary report lists totals for virus infections and message processing, as well as the specific viruses that were detected.

The report is organized as follows:

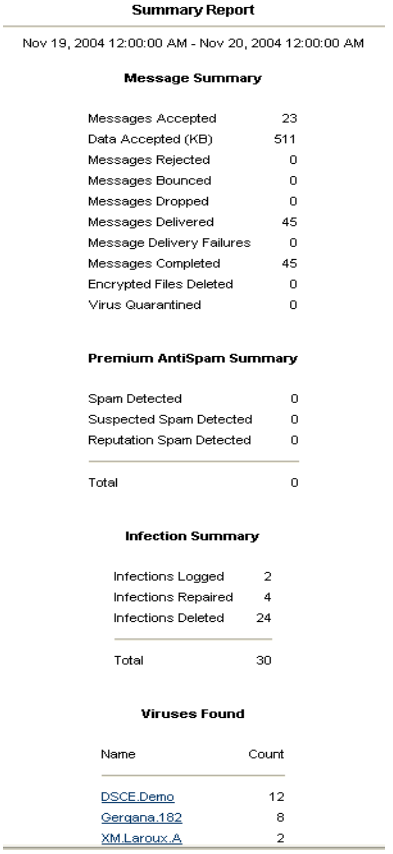
Message Summary	Shows totals for messages handled. See "About message summaries" on page 147.
Infection Summary	Shows totals for infections handled. See "About infection summaries" on page 148.

When there is data logged for these types of events, the report displays the following:

Viruses Found	Shows the virus name, the number of times that the virus was encountered during the designated time period, and the total number of viruses that were encountered. Selecting a virus name takes you to the Symantec Security Response Web site, where you can view specific data about the virus.
Subjects Blocked	Appears only when messages have been rejected due to blocked subject lines. It shows the subject line that triggered the block during the designated time period, a total for each blocked subject line, and a grand total. If a message meets more than one subject-line blocking criteria, if the message is to be dropped due to the subject violation, Symantec Mail Security for SMTP reports each subject violation in the detail report.
Spam Found	Appears only when the Symantec Premium AntiSpam license is valid. The summary report shows totals for spam, suspected spam, and reputation spam. If the Symantec Premium AntiSpam license is invalid, no spam information is reported.
Attachments Deleted	Shows the file names for attachments that were deleted during the designated time period, a total for each file name, and a grand total.

To generate summary reports

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Reporting**.
2. On the Summary Report tab, in the From and To drop-down lists, select the date and time range for the report.
3. Click **Generate Report**.



Summary Report

Nov 19, 2004 12:00:00 AM - Nov 20, 2004 12:00:00 AM

Message Summary

Messages Accepted	23
Data Accepted (KB)	511
Messages Rejected	0
Messages Bounced	0
Messages Dropped	0
Messages Delivered	45
Message Delivery Failures	0
Messages Completed	45
Encrypted Files Deleted	0
Virus Quarantined	0

Premium AntiSpam Summary

Spam Detected	0
Suspected Spam Detected	0
Reputation Spam Detected	0
Total	0

Infection Summary

Infections Logged	2
Infections Repaired	4
Infections Deleted	24
Total	30

Viruses Found

Name	Count
DSCE.Demo	12
Gergana.182	8
XM.Laroux.A	2

About message summaries

Table 7-2 lists the information that is included in the message summary section of a summary report.

Table 7-2 Message summary information

Action	Description
Messages accepted	Number of messages that were added to the fast queue
Data accepted (KB)	Cumulative size of messages
Messages rejected	Number of messages that were rejected because the software is configured to reject messages; disallowed characters are in an email address; an anti-relay violation occurs; the configured message size has been exceeded
Messages bounced	Number of incoming messages that were bounced
Messages dropped	Number of incoming messages that were dropped
Messages delivered	Number of outgoing messages that were delivered
Message delivery failures	Number of outgoing messages that were returned due to a delivery error
Messages completed	Number of messages that were processed by Symantec Mail Security for SMTP
Encrypted files deleted	Number of encrypted files that were deleted
Messages quarantined	Number of messages that were quarantined due to a virus

About Symantec Premium AntiSpam summaries

Table 7-3 lists the information that is provided in the Premium AntiSpam section of a summary report.

Table 7-3 Symantec Premium AntiSpam information

Action	Description
Spam detected	Number of spam messages detected
Suspected spam detected	Number of suspected spam messages detected
Reputation spam detected	Number of spam messages detected with the reputation service

About infection summaries

Table 7-4 lists the information that is provided in the Infection Summary section of a summary report.

Table 7-4 Infection summary information

Action	Description
Infections logged	Number of files logged
Infections repaired	Number of files that had viruses that were repaired
Infections deleted	Number of files that contained viruses that were deleted
Total infections	Number of viruses that were detected, repaired, deleted, and logged only

Generating detail reports

A detail report contains all of the events in the Symantec Mail Security for SMTP log. You can configure Symantec Mail Security for SMTP to log entries for various lengths of time.

See "Configuring logging options" on page 72.

The following are types of actions that can be included in a detail report:

- System: Associated with the operation of the Symantec Mail Security for SMTP server
  See "About system actions" on page 149.
- SMTP: Associated with the transmission of mail between the server that is running Symantec Mail Security for SMTP and other mail transfer agents (MTAs)
  See "About SMTP actions" on page 150.
- Symantec Premium AntiSpam: Associated with the premium antispam feature.
  See "About premium antispam actions" on page 151.
- Message: Associated with email processing
  See "About message actions" on page 152.
- Blocking: Associated with blocking messages
  See "About blocking actions" on page 153.

You can save the report in a comma-delimited (CSV) file format so that you can import it into spreadsheets or other graphical display software. The CSV report is saved in the log directory that was specified during installation (by default, the Windows location is \Program Files\Symantec\SMSSMTP\logs, and the Solaris location is /var/opt/SMSSMTP/logs). The report file name is SMSSMTPyyyymmddhhmm.CSV, which indicates the date and time of creation.

Note: There are legacy fields (Mailbox and Mailbox ID) that are in the CSV report that are no longer used and are always empty.

To generate a detail report

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Reporting**.
2. On the Detail Report tab, in the From and To drop-down lists, specify the date and time range for the report.
3. Check the actions to include in the report.
4. In the Search box, you can type a single search term or string to narrow the output of the report.
   The search is not case-sensitive.
   If no actions are checked, the report contains all of the entries from the log.
5. Select one of the following:
   - Generate Report
   - Write to CSV

About system actions

Table 7-5 lists the system actions.

Table 7-5 System actions

Action	Description
Logon	Shows the date and time of logon, the logon result (Succeeded/Failed), the user who logged on, and the user's client IP address
Logoff	Shows the date and time of logoff, the logoff result (Succeeded/Failed), the user who logged off, and the user's client IP address
LiveUpdate	Shows the date and time of the last LiveUpdate session and the LiveUpdate result (Succeeded/Failed)

Table 7-5 System actions

Action	Description
Definitions updated	Shows the date and time of the last virus definitions and spam definitions updates, the result of the updates (Succeeded/ Failed), and the date and revision number of the updates
Object modified	Shows the screen that was modified, date that information was changed through the administrative interface, what was modified, which user modified it and from which client, and the type of modification that was made
Service started	Shows the date and time that the Symantec Mail Security for SMTP service started
Service start failed	Shows the date and time that the Symantec Mail Security for SMTP service failed to start
Service stopped	Shows the date and time that the Symantec Mail Security for SMTP service stopped
Reordering started	Shows the date and time that queue reordering started
Reordering stopped	Shows the date and time that queue reordering stopped, the number of messages moved to the front of the queue, and the number of seconds spent performing a queue reorder

About SMTP actions

Table 7-6 lists the SMTP actions.

Table 7-6 SMTP actions

Action	Description
Connection from	Shows the date and time that any mail client attempted to connect to the Symantec Mail Security for SMTP server, the result of the connection (Succeeded/Failed), the client's IP address, and the connection ID
Connected to	Shows the date and time that the Symantec Mail Security for SMTP server attempted to connect to any mail server, the result of the connection (Succeeded/Failed), the connection ID, and connection information (Actual/Cached)
Disconnected	Shows which client or mail server was disconnected, the client ID, and the date and time of the disconnection

Table 7-6 SMTP actions

Action	Description
Connection closed	Shows the date and time that the connection was closed, the IP address of the server that connected to the Symantec Mail Security for SMTP server, the connection ID, the last command sent, and the last response sent by the disconnecting server
Protocol violation	Shows which client committed the violation, the connection ID, information about the protocol violation, and the date and time of the violation
Rejected	Shows that a message was rejected, which client it was rejected from, the date and time of the rejection, and the reason for the rejection

About premium antispam actions

Table 7-7 lists the premium antispam actions.

Table 7-7 Premium AntiSpam actions

Action	Description
Spam	Shows heuristic spam detection events and spam detection from the premium antispam service. The spam score for spam messages that are detected by the premium antispam engine will always report a score of 100.
Suspected spam	Shows only the Suspected Spam detection events for the premium antispam service. All messages that are detected as suspected spam will report a spam score of 89.
Reputation spam	Shows the events resulting from a match in the Open Proxy list. They will be treated as spam messages and will follow whichever disposition was set for spam messages.
Spam Quarantined	Shows information about the spam message that was quarantined (From, To, Subject, size, SMTP ID, date and time that message was quarantined).

About message actions

Table 7-8 lists the message actions.

Table 7-8 Message actions

Action	Description
Accepted	Shows the date and time that a message was accepted, the From/To information, the subject, the client IP address, the connection ID, and the SMTP ID
Dropped	Shows the date and time that a message was dropped, From/To information, the reason for the drop, and the SMTP ID
Forwarded	Shows the date and time that a message was forwarded, From/To information, the reason for the forward, and the SMTP ID
Bounced	Shows the date and time that a message was bounced, To information, the reason for the bounce, and the SMTP ID
Delivery failed	Shows the date and time that a message was delivered, the SMTP ID, and the last response of the server
Delivered	Shows the date and time that a message was delivered, From/To information, the client IP address, the connection ID, and the SMTP ID
Completed	Shows the date and time that the processing of a message was completed, the client IP address, and the SMTP ID
Delivery suppressed	Shows the date and time that a message was not delivered, From/To information, and the SMTP ID
Held	Shows the date and time that a message was placed in the hold queue, the sending client, To/From information, subject, size, SMTP ID, and the reason that the message was held
Quarantined	Shows the date that the file was quarantined in the Central Quarantine and the file name

About blocking actions

Table 7-9 lists the blocking actions.

Table 7-9 Blocking actions

Action	Description
Virus logged	Shows the date that the virus was logged, From/To information, and the virus name.
Files repaired	Shows the date that the file was repaired, From/To information, and the virus name.
Files deleted	Shows the date that the file was deleted, From/To information, and the virus name.
Subjects blocked	Shows the date that the subject was blocked, From information, subject, and which word or phrase was matched in the subject.
Scan error	Shows the date of the scan error, From/To information, and a description of the scan error.
Sender blocked	Shows the date and time of the block and the sender address.
Attachment deleted	Shows the matching file name, date and time that an attachment was deleted, From/To information, SMTP ID number, the name of the deleted file, and the reason for the file being deleted.
Spam list block	Shows the date and time that the message was blocked, how the message was handled, From/To information, SMTP ID, and the reason for the block.
Heuristic spam	Shows the date and time that the message was detected by the heuristic antispam engine, the IP address of the client that accepted the email message from Symantec Mail Security for SMTP, From/To information, subject, size of message (in bytes), SMTP ID, Info “Message is considered to be spam,” the spam definitions date, and the spam score. If a spam message is also malformed, the event will be reported only as malformed. (The report will not show a heuristic spam event for the message). **Note:** This setting will not display if the Symantec Premium AntiSpam license is valid.
Mass Mailer cleanup	Shows the date and time that the cleanup occurred, the sending client, From/To information, subject, size, SMTP ID, virus name, file name, and matching entry in MMC list.

Table 7-9 Blocking actions

Action	Description
Content rule violation	Shows the date and time that the violation occurred, the sending client, From/To information, subject, size, SMTP ID, and information for which the rule was triggered.
Spam rule violation	Shows the date and time that the violation occurred, the sending client, From/To information, subject, size, SMTP ID, and information for which the rule was triggered.

Chapter 8

Integrating Symantec Mail Security for SMTP with SESA

This chapter includes the following topics:

About SESA

In addition to using standard local logging for Symantec Mail Security for SMTP, you can also choose to log events to the Symantec Enterprise Security Architecture (SESA). SESA is an underlying software infrastructure and a common user interface framework. It integrates multiple Symantec Enterprise Security products and third-party products to provide a central point of control of security within an organization. It provides a common management framework for SESA-enabled security products, such as Symantec Mail Security for SMTP, that protect your IT infrastructure from malicious code, intrusions, and blended threats.

SESA helps you increase your organization's security posture by simplifying the task of monitoring and managing the multitude of security-related events and products that exist in today's corporate environments. SESA includes an event management system that employs data collection services for events generated

on computers that are managed by Symantec security products. The event categories and classes include antivirus, content filtering, network security, and systems management. The range of events varies depending on the Symantec applications that are installed and managed by SESA.

You can monitor and manage these security-related events through the SESA Console. The SESA Console is the common user interface that provides manageable integration of security technologies (Symantec or otherwise), Symantec Security Services, and Symantec Security Response. You can query, filter, and sort data to reduce the security-related events that you see through the SESA Console, which allows you to focus on threats that require your attention. You can configure alert notifications in response to events, and generate, save, and print tabular and graphical reports of event status, based on filtered views that you have created.

SESA must be installed and working properly before you can configure Symantec Mail Security for SMTP to log events to SESA.

For more information, see the SESA documentation.

Configuring logging to SESA

The logging of events to SESA is in addition to the standard local logging features for Symantec Mail Security for SMTP. Logging to SESA is activated independently of standard local logging. If you have purchased SESA, you can send a subset of the events that are logged by Symantec Mail Security for SMTP to SESA.

See "Interpreting Symantec Mail Security for SMTP events in SESA" on page 164.

To configure logging to SESA, you must complete the following steps:

- Configure SESA to recognize Symantec Mail Security for SMTP. In order for SESA to receive events from Symantec Mail Security for SMTP, you must run the SESA Integration Wizard that is specific to Symantec Mail Security for SMTP on each computer that is running the SESA Manager. The SESA Integration Wizard installs the appropriate integration components for identifying the individual security product (in this case, Symantec Mail Security for SMTP) to SESA.
  See "Configuring SESA to recognize Symantec Mail Security for SMTP" on page 157.

- Install a local SESA Agent on the computer that is running Symantec Mail Security for SMTP. The local SESA Agent handles the communications between Symantec Mail Security for SMTP and SESA.
  See "Installing the local SESA Agent using the SESA Agent Installer" on page 158.
- Configure Symantec Mail Security for SMTP (through the administrative interface) to communicate with the local SESA Agent and to log events to SESA.
  See "Configuring Symantec Mail Security for SMTP to log events to SESA" on page 164.

Configuring SESA to recognize Symantec Mail Security for SMTP

To configure SESA to receive events from Symantec Mail Security for SMTP, run the SESA Integration Wizard that is specific to Symantec Mail Security for SMTP on each computer that is running the SESA Manager. The SESA Integration Wizard installs the appropriate integration components for identifying Symantec Mail Security for SMTP to SESA. You must run the SESA Integration Wizard on each SESA Manager computer to which you are forwarding events from Symantec Mail Security for SMTP.

Each product that interfaces with SESA has a unique set of integration components. The integration components for all products that interface with SESA are available in the Symantec Mail Security for SMTP software distribution package.

See "Uninstalling the SESA Integration Package" on page 165.

To configure SESA to recognize Symantec Mail Security for SMTP

1. Do the following:
   - On the computer on which the SESA Manager is installed, insert the product CD.
   - Copy the SESA Integration Package (smssmtp.sip) to a location of your choosing.
2. On the Windows taskbar, click **Start** > **Programs** > **SESA** > **Register SESA Integrated Product**, and browse to the SESA Integration Package.

3 In the SESA Domain Administrator Information window, type the specific information about the SESA Domain Administrator and the SESA Directory.

SESA Domain Administrator Name	The name of the SESA Directory Domain Administrator account.
SESA Domain Administrator Password	The password for the SESA Directory Domain Administrator account.
Domain of SESA Directory	The domain of the computer on which the SESA Directory is installed.
Host Name or IP Address of SESA Directory	The IP address of the computer on which the SESA Directory is installed (may be the same as the SESA Manager IP address if both are installed on the same computer). If you are using authenticated SSL instead of SESA default, anonymous SSL, you must enter the host name of the SESA Directory computer. For example, mycomputer.com. For more information on SESA default, anonymous SSL and upgrading to authenticated SSL, see the *Symantec Enterprise Security Architecture Installation Guide*.
Secure Directory Port Host Name or IP Address	The number of the SESA Directory secure port. The default port number is 636.

4 Follow the on-screen instructions to install the appropriate SESA Integration Package and complete the SESA Integration Wizard.

5 Repeat steps 1-4 on each SESA Manager computer to which you are forwarding Symantec Mail Security for SMTP events.

Installing the local SESA Agent using the SESA Agent Installer

The local SESA Agent handles the communications between Symantec Mail Security for SMTP and SESA and is installed on the same computer that is running Symantec Mail Security for SMTP. The local SESA Agent is provided as part of the software distribution package for Symantec Mail Security for SMTP. A separate installation package for installing the Agent is located on the distribution CD for Symantec Mail Security for SMTP.

If you have more than one SESA-enabled product installed on a single computer, these products can share a local SESA Agent. However, each product must register with the Agent. Thus, even if an Agent has already been installed on the computer for another SESA-enabled security product, you must run the installer to register Symantec Mail Security for SMTP.

For more information, see the SESA documentation.

See "Configuring Symantec Mail Security for SMTP to log events to SESA" on page 164.

Install the local SESA Agent using the SESA Agent Installer

To install the SESA Agent using the SESA Agent installer that Symantec Mail Security for SMTP provides, run the Installer on all computers on which Symantec Mail Security for SMTP 4.1 is installed.

See "Uninstalling the local SESA Agent" on page 166.

To install the SESA Agent on Windows 2000 Server

1. Log on to the computer on which you have installed Symantec Mail Security for SMTP as administrator or as a user with administrator rights.
2. Copy the executable (.exe) file to install the Agent from the Symantec Mail Security for SMTP distribution CD onto the computer.
3. Run the .exe file.
4. On the Introduction page, click **Next**.
5. Indicate that you agree with the terms of the Symantec license agreement, and then click **Next**.
   If you indicate No, a warning is displayed. You must click **Quit** or **Resume**.
6. On the Readme page, read the information, and then click **Next**.
7. Under Choose Install Folder, select the location in which to install the local Agent, and then click **Next**.
   The default location is C:\Program Files\Symantec\SESA.
   If the SESA Agent is already installed on the same computer, this option does not display.
8. From the list of products, choose one or more with which the Agent will work.

9 In the Primary SESA Manager IP address or host name box, type the IP address or host name of the computer on which the primary SESA Manager is running.
If SESA is configured to use anonymous SSL (the default setting), type the IP address of the primary SESA Manager. If SESA is configured to use authenticated SSL, type the host name of the primary SESA Manager (for example, computer.company.com).

10 In the Primary SESA Manager port number box, type the port number on which the SESA Manager listens.
The default port number is 443.

11 If you are running a Secondary SESA Manager that is to receive events from Symantec Mail Security for SMTP, do the following:

- In the Secondary SESA Manager IP address or host name box, type the IP address or host name of the computer on which the Secondary SESA Manager is running.
- In the Secondary SESA Manager port number box, type the port number on which the Secondary SESA Manager listens.
  The default port number is 443.

12 In the Organizational unit distinguished name box, type the organizational unit distinguished name to which the Agent will belong.
If the organizational unit is unknown or not yet configured, you can leave this setting blank. Use the format shown in the following example:
ou=Europe,ou=Locations,dc=SES,o=symc_ses
The domain(s) (dc=) portion of the path should correspond to the domain that is managed by the selected SESA Management Server.

13 Select one of the following:

- Start SESA Agent Automatically: The SESA Agent starts automatically whenever the computer is restarted.
- Start SESA Agent Manually: You must manually restart the SESA Agent each time that the computer is restarted.

14 Check **Start the SESA Agent at installation completion** if you want the SESA Agent to start immediately after the installation finishes.
If you do not check the check box, you must manually start the SESA Agent after the installation is complete.

15 On the Pre-Installation Summary page, verify that all information is correct, and then click **Install**.
The installer proceeds from this point with the installation. When the installation is complete, the Agent is installed as a Windows 2000 service and is listed as SESA AgentStart Service in the Services Control Panel.

To install the SESA Agent on Solaris

1. Copy the bin (.bin) file to install the Agent from the Symantec Mail Security for SMTP distribution CD onto the computer, and change directories to the location where you copied the file.
2. Log on as root to the computer on which you have installed Symantec Mail Security for SMTP.
3. Do one of the following:
   - To use the graphical interface for installing on Solaris, at the command prompt, type the following command:
     ```
     ./sesa_agent_installer -i gui
     ```
     Follow the instructions for Windows installation. Change the default location to /opt/Symantec/Sesa
   - At the command prompt, type the following command to run the Agent Installer file from the Symantec Mail Security for SMTP distribution CD, and then press **Enter**:
     ```
     ./sesa_agent_installer.bin
     ```
4. On the Introductory page, click **Enter**.
5. Indicate that you agree with the terms of the Symantec license agreement, and then click **Enter**.
   If you indicate No, the installation is cancelled.
6. On the Readme page, read the readme file, and then click **Enter**.
7. Select the location in which to install the SESA Agent, and then click **Next**.
   The default location is /opt/Symantec/sesa.
   If the SESA Agent is already installed on the same computer, this option does not display.
8. From the list of numbered list of products to register with SESA, type the number for each product that you want to register.
   Numbers must be separated by commas with no spaces between.
9. Do one of the following:
   - Type the IP address or host name of the computer on which the primary SESA Manager is running.
     If SESA is configured to use anonymous SSL (the default setting), type the IP address of the primary SESA Manager. If SESA is configured to use authenticated SSL, type the host name of the primary SESA Manager (for example, computer.company.com).
   - Type the port number on which the SESA Manager listens.
     The default port number is 443.

10 If you are running a Secondary SESA Manager that is to receive events from Symantec Mail Security for SMTP, do the following:
   - Type the IP address or host name of the computer on which the Secondary SESA Manager is running.
   - Type the port number on which the Secondary SESA Manager listens. The default port number is 443.

11 Type the organizational unit distinguished name to which the Agent will belong.
   If the organizational unit is unknown or not yet configured, you can leave this setting blank. Use the format shown in the example:
   ou=Europe,ou=Locations,dc=SES,o=symc_ses
   The domain(s) (dc=) portion of the path should correspond to the domain that is managed by the selected SESA Management Server.

12 Type one of the following to indicate whether the SESA Agent should start automatically on system boot:
   - 1: The SESA Agent starts automatically on system boot.
   - 2: You must manually restart the SESA Agent after each system boot.

13 Type one of the following to indicate whether the SESA Agent should start immediately after the installation finishes:
   - 1: The SESA Agent starts immediately after installation.
   - 2: You must manually start the SESA Agent after installation.

   The installer proceeds from this point with the installation. Unless you indicated otherwise during the installation, the SESA Agent starts automatically when the installation is complete. You may need to stop and restart the SESA Agent. A transcript of the installation is saved as /var/log/SESAAGENT-install.log for later review.

Installing the SESA Agent manually by command line

As an alternative to using the SESA Agent Installer, you can install the SESA Agent by command line.

Install the SESA Agent manually by command line

To install the SESA Agent, you do the following:

- Prepare to install the SESA Agent.
- Install the SESA Agent by command line.

To prepare to install the SESA Agent

1. On the computer on which Symantec Mail Security for SMTP is installed, create a folder for the SESA Agent files.
   For example, C:\Agent.
2. Insert the SESA CD1 - SESA Manager into the CD-ROM drive.
3. Copy the files from the \Agent folder on the CD and paste them in the newly created folder on the Symantec Mail Security for SMTP computer.
4. In a text editor, open the Agent.settings file.
   For example, C:\Agent\Agent.settings.
5. Change the value of the mserverip setting to the IP address of the SESA Manager to which Symantec Mail Security for SMTP will forward events.
6. Save and close the Agent.settings file.

To install the SESA Agent by command line

1. On the computer on which Symantec Mail Security for SMTP is installed, at the command prompt, change to the folder in which the SESA Agent files reside.
   For example, C:\Agent.
2. At the command prompt, type the following:
   `java -jar agentinst.jar -a3067`
   3067 is a unique product ID to install the Agent for Symantec Mail Security for SMTP. To remove the SESA Agent, you must use the same product ID parameter (for Symantec Mail Security for SMTP, 3067).
   Optionally, you can append any of the following parameters:

-debug	Writes logging information to the screen
-log	Turns off the installation log and instructs the SESA Agent to write logging information to the Agntinst.log file in the local Temp directory

Configuring Symantec Mail Security for SMTP to log events to SESA

After you have installed the local SESA Agent to handle communications between Symantec Mail Security for SMTP and SESA, you must configure Symantec Mail Security for SMTP to communicate with the Agent. You must also ensure that logging to SESA has been activated. These settings are located on the Symantec Mail Security for SMTP administrative interface.

To configure Symantec Mail Security for SMTP to log events to SESA

1. On the Symantec Mail Security for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Logging tab, under SESA logging, check **Enable SESA logging**.
3. Click **Save Changes**.

Interpreting Symantec Mail Security for SMTP events in SESA

SESA provides extensive event management capabilities, such as common logging of normalized event data for SESA-enabled security products like Symantec Mail Security for SMTP. The event categories and classes include antivirus, content filtering, network security, and systems management. SESA also provides centralized reporting capabilities, including graphical reports. The events that are forwarded to SESA by Symantec Mail Security for SMTP take advantage of the existing SESA infrastructure for events.

You can create alert notifications for certain events. Notifications include pagers, SNMP traps, email, and operating system event logs. You can define the notification recipients, day and time ranges when specific recipients are notified, and custom data to accompany the notification messages.

For more information on interpreting events in SESA and on the event management capabilities of SESA, see the SESA documentation.

Uninstalling the SESA Integration Package

To uninstall the SESA Integration Package, you must run the SESA Integration Wizard on each SESA Manager computer that is receiving events from Symantec Mail Security for SMTP 4.1.

To uninstall the SESA Integration Package

1. Do the following:
   - On the computer on which the SESA Manager is installed, insert the product CD.
   - Copy the SESA Integration Package to a location of your choosing.
2. On the Windows taskbar, click **Start** > **Programs** > **SESA** > **Unregister SESA Integrated Product**, and browse to the SESA Integration Package.
3. In the SESA Domain Administrator Information window, type the specific information about the SESA Domain Administrator and the SESA Directory.

SESA Domain Administrator Name	The name of the SESA Directory Domain Administrator account.
SESA Domain Administrator Password	The password for the SESA Directory Domain Administrator account.
Domain of SESA Directory	The domain of the computer on which the SESA Directory is installed.
Host Name or IP Address of SESA Directory	The IP address of the computer on which the SESA Directory is installed (may be the same as the SESA Manager IP address if both are installed on the same computer). If you are using authenticated SSL instead of SESA default, anonymous SSL, you must enter the host name of the SESA Directory computer. For example, mycomputer.com. For more information on SESA default, anonymous SSL and upgrading to authenticated SSL, see the *Symantec Enterprise Security Architecture Installation Guide*.
Secure Directory Port Host Name or IP Address	The number of the SESA Directory secure port. The default port number is 636.

4 Follow the on-screen instructions to uninstall the appropriate SESA Integration Package.

5 Repeat steps 1- 4 on each SESA Manager computer to which you are forwarding Symantec Mail Security for SMTP events.

Uninstalling the local SESA Agent

The local SESA Agent is automatically uninstalled when you uninstall Symantec Mail Security for SMTP. If more than one product is using the Agent, the uninstall script removes only the Symantec Mail Security for SMTP registration and leaves the Agent in place. If no other security products are using the Agent, the uninstallation script will uninstall the Agent as well.

You can also uninstall the Agent from Windows through the Control Panel.

To uninstall the local SESA Agent from Windows through the Control Panel

1 On the Windows taskbar, click **Start** > **Settings** > **Control Panel** > **Add or Remove Programs** > **SESA Agent**.

2 Click **Change/Remove**.

3 Click **Uninstall**.

4 Read the warning, and then click **Uninstall the SESA Agent**.
If more than one product is using the Agent, selecting this option will uninstall the Agent from all of the products.

5 Click **Done**.

To uninstall the local SESA Agent from Solaris by running a script

1 Do one of the following:

- To use the graphical interface for uninstalling on Solaris, at the command prompt, type the following command:
  `./sesa_agent_uninstaller -i gui`
- Change to the installation directory.
  The default directory location is
  /opt/Symantec/Sesa/Uninstall_SESA Agent

2 Type the following command:
`./Uninstall_SESA_Agent`

3 Read the readme information, and then click **Enter**.

4 Click **Done**.

Index

T

U

V

W

Symantec Mail Security™ for SMTP

CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: _____ CD Replacement(s)
Name _____
Company Name _____
Street Address (No P.O. Boxes, Please)_____
City _____ State _____ Zip/Postal Code _____
Country* _____ Daytime Phone _____
Software Purchase Date_____
*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.
Briefly describe the problem:_____

CD Replacement Price	$ 10.00	SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.
Sales Tax (See Table)	_____	
Shipping & Handling	$ 9.95	
TOTAL DUE	_____	

FORM OF PAYMENT ** (Check One):

___ Check (Payable to Symantec) Amount Enclosed $ _____ _____ Visa _____ Mastercard _____ AMEX
Credit Card Number _____ Expires _____
Name on Card (please print) _____ Signature _____
**U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
555 International Way
Springfield, OR 97477 (800) 441-7234
Please allow 2-3 weeks for delivery within the U.S.